ARL-TR-7451 ● SEP 2015

US Army Research Laboratory

Network Science Experimentation Vision

by David Alberts, Alexander Kott, Brian Rivera, Kevin Chan, Lisa Scott, Reginald Hobbs, Alice Leung, Will Dron, and Ritu Chadha

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-TR-7451 ● SEP 2015

US Army Research Laboratory

Network Science Experimentation Vision

by David Alberts
Institute for Defense Analysis

Alexander Kott, Brian Rivera, Kevin Chan, Lisa Scott, and Reginald Hobbs
Computational and Information Sciences Directorate, ARL

Alice Leung and Will Dron
BBN

Ritu Chadha
Vencore Labs, Incorporated

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
September 2015	Final	

4. TITLE AND SUBTITLE
Network Science Experimentation Vision

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
David Alberts, Alexander Kott, Brian Rivera, Kevin Chan, Lisa Scott, Reginald Hobbs, Alice Leung, Will Dron, and Ritu Chadha

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army Research Laboratory
ATTN: RDRL-CIN
2800 Powder Mill Road
Adelphi, MD 20783-1138

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-7451

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The success of military operations has been shown to depend upon the capabilities and performance of a heterogeneous collection of interdependent networks. This report outlines and discusses an experimentation vision that identifies and organizes a set of research activities and the experimentation ecosystem necessary to improve our understanding of these multi-genre composite networks.

15. SUBJECT TERMS
networks, experiments, cyber security, network performance, c2

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr Alexander Kott
Unclassified	Unclassified	Unclassified	UU	80	19b. TELEPHONE NUMBER (Include area code) 301-394-1507

Contents

List of Figures

List of Tables

INTENTIONALLY LEFT BLANK.

1. Introduction

The success of military operations has been shown to depend upon the capabilities and performance of a heterogeneous collection of interdependent networks. Such a collection of networks is referred to here as a multi-genre composite network. Given that the term "network" is used in a multiplicity of ways in a variety of contexts, it is important to state that it is used in this report in its most basic and inclusive meaning, that is, as a collection of connected nodes. This definition includes all manner of nodes and the links that allow these nodes to interact with one another. Thus, this use of the term network encompasses not only the technical networks associated with cyberspace (communications and information networks), but also social networks, the principal ones being the command and control (C2) networks whose characteristics and behaviors are shaped by the approach to C2 adopted for a military operation.

Experiments and case studies that have looked at C2 approaches and systems performance in the context of a variety of missions and circumstances have conclusively shown that there is no single best approach to C2. These experiments and case studies also show that the most appropriate approach to C2 (solution to overall composite network design problem) is a function of the nature of the mission and circumstances.[1] These findings suggest a number of hypotheses related to multi-genre composite networks. First, there is no single best approach to designing and operating the communications and information networks that support C2. Second, to "optimize" C2 Agility, one needs to "optimize" the agility of the composite network. Third, the agility of one network can, at least in part, compensate for a lack of agility of an interdependent network. Thus, in addition to the appropriate selection of a C2 Approach, one needs to simultaneously consider a set of design choices for the supporting communication and information networks. In other words, one should seek an integrated design of the composite network.

Given the well-established link between the behaviors, performance, and agility of Army networks and mission success, it is critical for us to test these hypotheses and improve our understanding of and our ability to design, assure, and command and control the Army Composite Network. This serves to ensure the appropriate levels of performance under a variety of conditions and circumstances.

1.1 Purpose of Report

This report outlines and discusses an experimentation vision that identifies and organizes a set of research activities designed to improve our understanding of the composite networks that are critical for successful military operations.

The Army recently convened a workshop to envision the battlefield of 2050.[2] Workshop participants painted a picture of an overcrowded battlefield populated by all manner of robots, a battlefield where robots greatly outnumber human fighters. They concluded that the decisive edge would go to the adversary that had the most effective combined armies of humans and robots. They observed that these networked entities would act with varying degrees of autonomy to 1) collect, process, and disseminate information to develop situational awareness; 2) direct and manage collections of robots that were engaged in executing C2, combat-support functions, as well as combat missions; and 3) undertake a full range of defensive and offensive cyber operations.

Among the key findings of this workshop was the critical importance of being able to command and control this collection of humans, enhanced humans, and a variety of physical and cyber robots. Our ability to design, deploy, and manage composite networks will determine how effective and how agile our networked armies will be, and hence, whether we have a decisive advantage. Workshop participants also noted that given the importance of robots, both physical and virtual, these entities would be subject to a variety of attacks, and hence, composite network security (protection and assurance of communications, information, and computers from cyber-attacks) would be a key factor in determining the adversary with the competitive advantage.

The goal of the envisioned experiments and related analyses is to help the Army improve the capabilities and performance of not only the individual networks that are part of the Army Composite Network, but also to enable the Army to undertake an integrated design of the composite network, a design that considers the tradeoffs in characteristics and performance between and among these various networks necessary to improve their collective agility, that is, their ability to be successful over a wide range of mission, circumstances, and conditions. These tradeoffs involve the critical considerations associated with the integration of autonomous systems and entities and cybersecurity. Improvements in composite network performance and agility will increase the likelihood of success under a variety of missions, circumstances, and stresses that are associated with austere, hostile, and contested environments.

1.2 Organization of the Report

This report begins with an overview of the experimentation ecosystem required to support the research needed to understand and shape the behaviors of militarily relevant composite networks. The critical elements of such an ecosystem are identified and described. These include a Campaign of Experimentation (CAMPX) that involves the development of a conceptual model; a series of model-driven experiments; a data repository that contains the results of experiments and analyses

of the data; an experimentation infrastructure; and a community of researchers. The importance of ecosystem management and the benefits of an experimentation ecosystem conclude this section of the report. This general discussion of an experimentation ecosystem is followed by a discussion of a multi-threaded campaign of experiments designed to mature our understanding of militarily relevant composite networks that feature the identification of hypotheses and metrics as well as descriptions of three initial experiments. The first of these experiments, Experiment 1, is designed to show that it is feasible, within existing capabilities and facilities, to design and conduct composite network experiments that can explore the interdependencies between and among networks of different genres. The second experiment involves the addition of a third network and an ability to monitor individual and composite network performance to inform dynamic adaption. The final experiment described focuses on being able to integrate cybersecurity measures, metrics, and hypotheses into previous experiments. The report concludes with a proposed way ahead.

2. Experimentation Ecosystem

The Army Composite Network, as a result of the myriad interdependencies that exist within and between and among its component networks and the roles that humans and automation play, is a complex, adaptive system. Understanding its dynamic behaviors and the impact that design choices will have requires an interdisciplinary team and a systematic approach. The ecosystem specified below provides this diverse set of researchers with the organization and tools they need to make progress in this very challenging endeavor.

The ecosystem envisioned consists of the following 3 mutually supportive components:

- Multi-thread CAMPX
- An accessible experimentation infrastructure
- Community of researchers

A multi-thread CAMPX provides the conceptual framework necessary to identify and prioritize the experiments that are needed to improve our current understanding, which will evolve as the campaign unfolds. It also provides the structure necessary to organize existing theories and the collection of experimental results that can be used to test these theories.

Experience has shown us that our experimentation efforts are limited by the research infrastructure that is available to researchers. Although progress is being made on the construction of venues that can be employed to investigate composite

networks, current capabilities in this regard are very limited and cannot support the experimentation envisioned in this report.

It is not enough to simply recruit researchers from different disciplines to tackle aspects of the composite network problem. These researchers need to interact and collaborate with one another on an ongoing basis. That is, they need to be members of a research community that can support realistic and militarily relevant experimentation.

Each of these 3 components of the ecosystem is discussed in more detail below.

2.1 Multi-thread Campaign of Experimentation

A CAMPX is a managed set of model-driven experiments and analyses designed to mature our understanding of a concept or capability of interest, in this case, militarily relevant composite networks.

2.1.1 Need for a CAMPX

The complexity of composite networks and the multitude of factors that impact the dynamics of their interactions make it infeasible to explore their interdependencies without undertaking a well-designed and well-supported multi-threaded CAMPX. This is due to the nature of individual experiments:

- Have a limited focus
- Consider a relatively small subset of the relevant variables
- Need to choose between high fidelity and large number of runs
- Include untested assumptions
- Lack independent verification
- Cannot adequately deal with random effects
- Produce findings “that depend upon…”

CAMPXs, however, can systematically consider the full range of factors that may impact composite network performance in a variety of situations and circumstances employing a variety of environments.

Table 1 compares the characteristics, attributes, and abilities of a single experiment with a CAMPX.

Table 1 Experiment v. CAMPX

Experiment	CAMPX
observe a phenomenon or test a hypothesis under a set of circumstances	explore a multi-faceted phenomenon moving beyond description to understanding, prediction, and ultimately, control
a single event a single model a single venue	multiple events multiple models multiple venues with increasing fidelity and relevance over time
considers a limited number of variables	explores a large number of variables and combinations of factors
produces limited data	accumulates a significant amount of data over time
analysis limited to data produced	analysis 'independent' of any one experiment and draws upon accumulated evidence
needs to be validated	incorporates integrated validation
relatively inefficient	very efficient

Source: Adapted from DoDCCRP Code of Best Practice Experimentation Figure 4.1

2.1.2 CAMPX Overview

Experimentation campaigns consist of the set of activities and products depicted in Fig. 1.

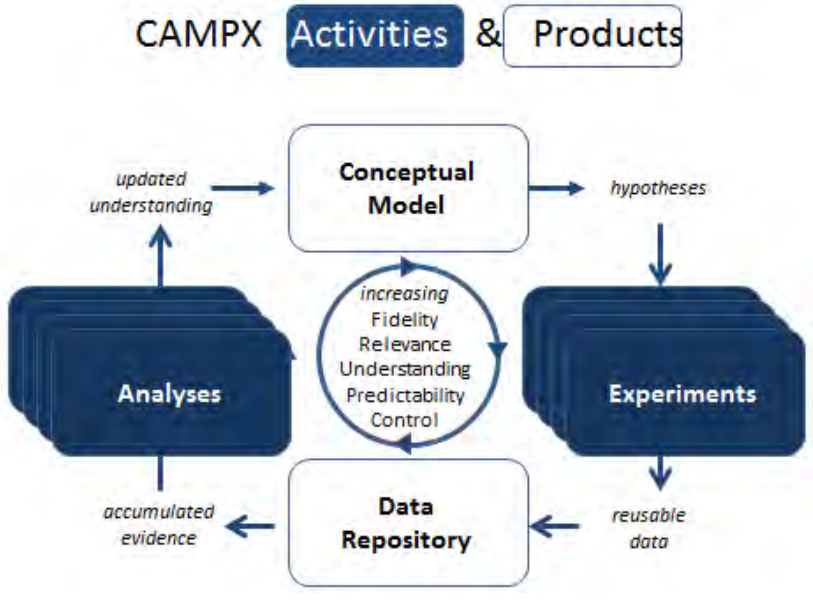

Fig. 1 CAMPX activities and products

These activities and products are produced in an iterative fashion, each iteration designed to increase fidelity, military relevance, our understanding and ability to predict, and our ability to control the collection of mission-critical networks.

2.1.3 Conceptual Model

The conceptual model is central to the design and conduct of a CAMPX. It identifies the key variables that are thought to significantly impact design, performance, and value. It specifies the nature of the relationships between and among these variables and identifies the "controllable" variables. The conceptual model also establishes metrics and articulates the value chain from the controllable variables to measures of enterprise value. Explicitly identifying these variables and relationships serve to both document and organize current understanding. It provides a context for individual theories, capabilities, research, and analysis and a way of measuring progress (maturation of understanding.) By identifying gaps in our understanding, the conceptual model suggests the hypotheses that drive and shape further experimentation and analysis.

The conceptual model for the envisioned multi-threaded CAMPX needs to include an Endeavor Space model, a set of single-genre network models, a composite network model, a cybersecurity network model, and a composite value chain that provides the links between design parameters and metrics associated with mission performance. A detailed discussion of the conceptual model and these "sub" models can be found in Section 4.3.

2.1.4 Experiments

During the course of a CAMPX, the nature of the experiments undertaken will evolve as understanding is gained. Thus, experiments will differ in their focus, scope, granularity, level of fidelity, and the extent to which the variables of interest can be controlled. As a result of these factors, the experiments conducted will, over time, differ with respect to the nature of the data they produce. It should be expected that the experimental infrastructure will need to evolve as well to support these experiments.

In the early stages of a CAMPX, it is common that "exploratory" experiments are designed and conducted to identify first-order variables that impact behaviors and outcomes. These results of these exploratory experiments are used to help determine what variables need to be accounted for during "follow-on" hypothesis testing experiments. Exploratory experiments are also used to see if experimental protocols work. For example, are controllable variables really controllable? Are participants conversant with their assigned responsibilities and the systems that are a part of the experiment? These experiments are also a good place to validate our data collection instruments to ensure that they collect the data needed for the analysis.

After an initial round of exploratory experiments, the CAMPX shifts to "hypothesis testing" experiments. These experiments are designed to ascertain if the relationships believed to exist between and among the variables do, in fact, exist

and provide additional information about these relationships including whether or not some relationships are conditional, that is, if they depend upon intervening variables. For example, $Y = f_1(X)$ when $a < Z < b$.

As a result of both the exploratory and hypothesis testing experiments, we will have an updated conceptual model that can be used to design experiments that explore the relationships between controllable variables (in this case, network the design parameters for the communications and information networks and C2 approaches for the social/C2 networks) and both individual network performance metrics and composite network metrics.

After the relationships between various design and performance variables has been established over a variety of conditions, the CAMPX is now is a position to move on to "intervention" experiments. These experiments are designed to see if dynamic manipulations of design parameters can achieve the desired results. In this case, can dynamic design improve network performance and translate into better mission outcomes. These experiments provide us with opportunities to see if we can turn our understanding of network behaviors into an ability to actually influence behaviors and outcomes.

In the final stages of a CAMPX, efforts are increasingly focused upon conducting "demonstration" experiments to create awareness of what has been achieved and building the confidence needed to move what we have learned in experimental settings into concept development, doctrine and operations.

The progression from exploratory experiments to hypothesis testing experiments, and then to experiments that explore how design parameters can be used to shape network behaviors and outcomes requires that these experiments increase their fidelity. Fidelity refers to the extent to which a model or an experiment is able to replicate reality. More realistic experiments can generate higher quality data, which, in turn, can be used to improve the fidelity of a conceptual model and the maturity of our understanding. Increased understanding improves our ability to predict and ascertain the potential value of changes in network capabilities and C2 approaches.

The factors affecting the fidelity of an experiment include the following:

- how entities, processes, and the operating environment are represented
- the nature of the assumptions (explicit and implicit)
- the set of variables and how they are observed, controlled, and measured

2.1.5 Data Repository

Given the number of variables that have a significant impact upon the performance of individual networks and the composite network, a great deal of data is needed to reach a critical mass for analysis and statistical significance. To reach this critical mass, results from a number of experiments need to be combined. To both document the experiments that have been undertaken, facilitate the reuse of the empirical results, and amass enough data for meaningful analysis, the conduct of a CAMPX requires a widely accessible data repository.

Having a data repository, in and of itself, is not sufficient. In order to reuse and appropriately combine data from different experiments, the data produced need to employ common or compatible metrics and also need to be tagged with appropriate metadata. Thus, the experiments that are part of a CAMPX need to be designed and instrumented to maximize reuse. Infrastructure-provided compatible transaction log generators facilitate the accumulation and reuse of experimental results that can support a variety of analyses. By focusing subsequent experiments to fill in gaps and/or generate larger sample sizes, needed research is enabled and can be conducted more efficiently.

2.1.6 Analyses

The concept and conduct of a CAMPX involves breaking the link between an experiment and the analysis, effectively transferring "ownership" of data from individual researchers to the community, thereby building richer sets of data and making them more widely available. The ability to take advantage of data from multiple experiments increases sample sizes, fleshes out factorial designs, facilitates sensitivity analyses, and facilitates cross-analysis comparisons. Infrastructure-provided log analyzers increase the quality and compatibility of analysis findings while reducing the time and costs of analysis.

2.1.7 Need for Multiple Threads

Militarily relevant composite networks consist of individual networks of different genres. Each genre is associated with different kinds of nodes and interactions between and among these nodes as well as different sets of design parameters and a different value chain. Thus, understanding composite networks involves not only understanding the interdependencies that exist between and among its component networks, but also the behaviors of these individual networks and the relationships between their design and value. In order to explore their behaviors and increase our understanding of these behaviors, these require their own CAMPX thread.

In addition, there are a set of questions to be addressed regarding securing and assuring these networks. There is a set of questions that apply to each of the genre-specific networks and a set that applies to them collectively. Finally, the

performance of these networks is not an end in itself but an enabler of mission performance. Therefore, there needs to be a campaign thread that addresses the overall behavior and performance of the collection of networks and their instantiation of cybersecurity measures.

Figure 2 depicts the multi-thread CAMPX envisioned to explore the design and behaviors of militarily relevant composite networks.

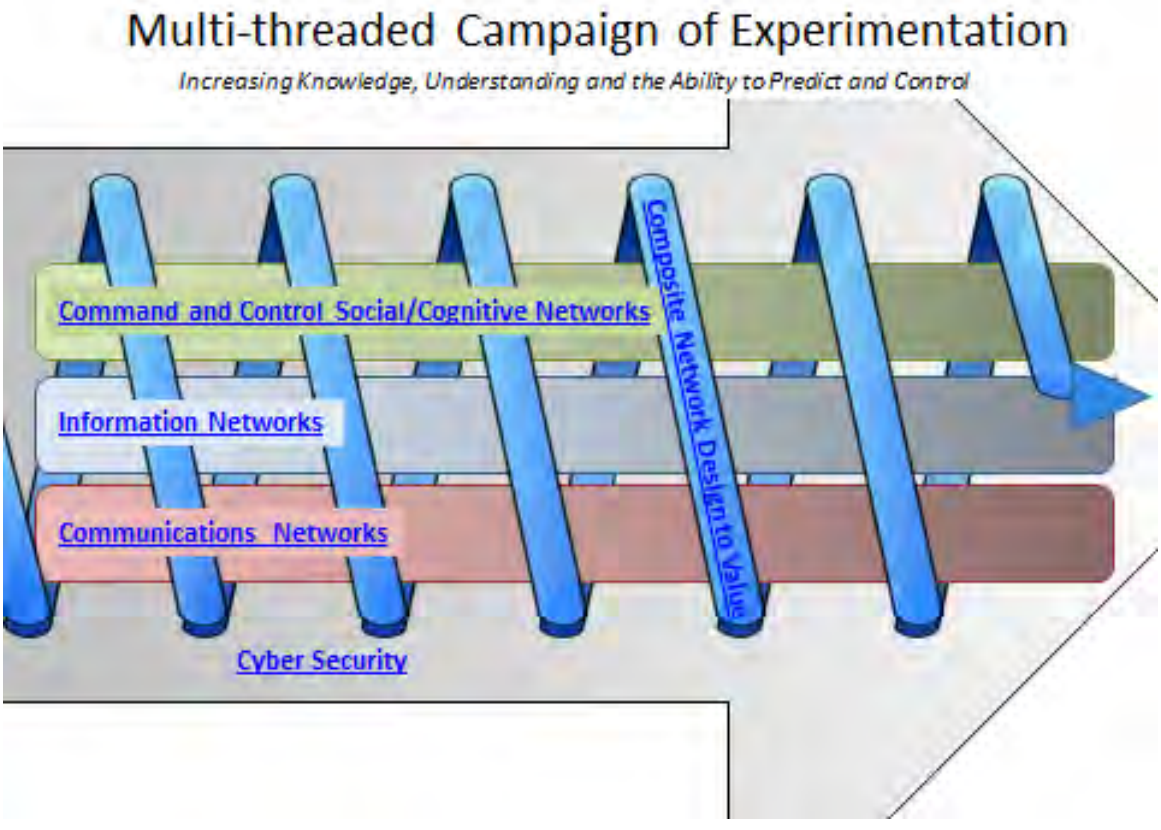

Fig. 2 Multi-threaded CAMPX

2.2 Experimentation Infrastructure

Figure 3 puts the experimentation infrastructure in the context of a CAMPX. In a CAMPX, it is the conceptual model that drives experiments, not the capabilities or lack thereof, provided by a given experimentation infrastructure.

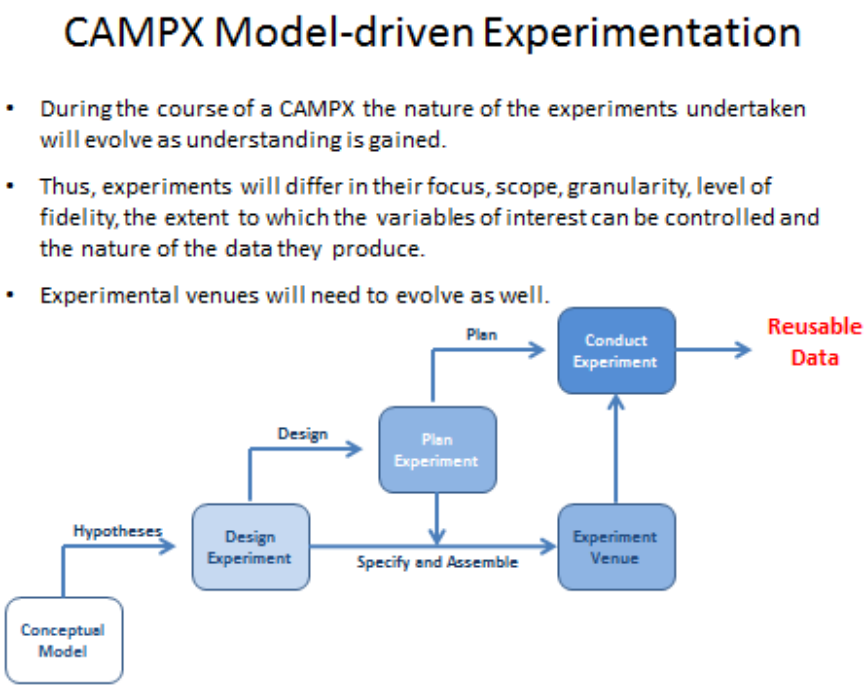

Fig. 3 CAMPX model-driven experimentation

The lack of a suitable experimentation infrastructure can scuttle a CAMPX before it is able to launch. Good experimental design means little if it cannot be realized in an actual experiment, and meaningful analysis cannot be achieved without appropriate data, data that, for the most part, need to be captured by the experimentation infrastructure. Of course, having an infrastructure that is not widely accessible to the community of researchers also constrains the ability of the CAMPX to achieve its objectives (see Section 4).

The ability of an experimentation infrastructure to support model-driven experiments is a function of its instrumentation capabilities, its plug and play features, and its visualization and analysis tools. There are a set of key capabilities that an experimentation infrastructure must have in order to support explorations into the behaviors and design considerations for militarily relevant composite networks. The infrastructure must be capable of representing the dynamic interactions between and among interdependent communications, information, and cognitive/social networks. It must have an "inventory" of plug and play components that allow researchers to explore a variety of theories and prototype capabilities in a dynamic composite network environment. The experimentation venues that are part of the experimentation infrastructure must be able to produce detailed transaction logs that can be independently analyzed. Furthermore, the infrastructure must support multiple simultaneous experiments and analyses.

A detailed discussion of the infrastructure, and its initial operating capabilities, can be found in Section 4.5.

2.3 Research Community

Developing an understanding of the behaviors associated with mission-focused composite networks requires a diverse community of researchers with expertise in a number of disciplines and experience in applying their requisite expertise, models, and tools in multiple domains. These areas of expertise include, but are not limited to, the following:

- networks and network architectures in general
- communications networks (fixed and mobile)
- information networks
- data, information, and knowledge management
- social networks
- C2 approaches, processes, and networks
- military and intel doctrine and operations
- cybersecurity and risk management
- human cognition
- organization theory
- social, team, and crowd behaviors
- human-machine interfaces
- automation and software agents
- modelling and simulation
- experimentation
- analysis

A community, in the context of a CAMPX, is more than simply a collection of researchers. It requires sustained and in-depth collaborations with interdisciplinary teams. It assumes that individuals with the above list of expertise and skills will be involved. This, in turn, requires getting a number of Army, academic, and industry organizations involved. The US Army Research Laboratory (ARL) has 2 major collaborative research efforts underway: one for network science and the other for cybersecurity. These have been able to attract individuals and organizations working in many of the areas listed above. In addition, ARL has a diverse staff of researchers upon which to draw. To augment this collection of researchers, ARL will need to reach out to the Command and Control Research community (CCRP),

the Military Operations Research (MORS) community, and the Organizational Design (OD) community.

2.4 Ecosystem Leadership Management

Leadership is required to establish the focus of CAMPX threads, provide an initial conceptual model and metrics, establish an appropriate research infrastructure, and when required, sponsor specific research collaborations. Management and oversight is required to ensure that a phased CAMPX Plan is developed and is adapted as the campaign unfolds. Management is also required to ensure that an accessible data repository is established and updated with the data obtained from experiments and that the conceptual model is updated to reflect the findings of both experimental and meta-analyses. Oversight of other aspects of the CAMPX need to occur to make sure that there is an appropriate mix of experiments and analyses and that these are appropriately designed and conducted.

ARL, working with other Department of Defense (DOD) organizations, industry, and academia needs to develop an appropriate approach to Collective C2 for the conduct of CAMPX and the provision of the associated Experimentation Ecosystem.

3. Experimentation Ecosystem Payoffs

The value of the Experimentation Ecosystem described in this report is hard to overstate. Without such an ecosystem, the systematic exploration of complex composite network behaviors necessary to develop an understanding of their implications for military missions and organizations would require significantly larger investments of time and resources. The different components of the Ecosystem make specific contributions that enable research that is currently beyond the reach of current researchers to be accomplished in an efficient and effective manner.

3.1 Research Enabled by Multi-Threaded CAMPX

Composite networks, by their very nature, involve dynamic interactions between and among networks of different genres. Army composite systems are purposeful and the ability to exercise C2 is a primary consideration. Given that C2 decisions shape and constrain the behaviors of Army networks, C2 decisions need to be informed by an understanding of the impacts that various design and policy options have on composite network behaviors. Among the C2 decisions that will become both more necessary and more critical in the years to come are those related to autonomous systems and entities. Critical composite network capabilities such as cybersecurity cannot be designed or assessed without taking into consideration

dynamic cross-genre interactions and the tradeoffs involved. As a result, they produce complex behaviors that cannot be adequately reproduced with single-genre network experiments or even 2-genre networks. Therefore, the observations and conclusions from the research and/or experiments that do not involve the simulation or observation of a composite network cannot provide the Army with the understandings they need to design and develop militarily relevant composite networks. Readers should not infer that single-genre or even sub-genre research is not necessary; it is. Rather, the point is that this research needs to be complemented by composite network research to inform design tradeoffs.

Should the Army rely solely on the results of single-genre experimentation to select design parameter values for each of the single-genre networks that constitute a composite network, these network designs would in all likelihood result in sub-optimal composite network performance. There is also a significant chance that dysfunctional behaviors and less than acceptable performance will result under certain conditions.

Despite the obvious need to look at composite networks holistically, there are a number of impediments that researchers currently face in trying to experiment with militarily relevant composite networks:

- identifying the complete set of relevant variables and relationships
- controlling the variables of interest
- stimulating, simulating, and/or observing the behaviors of interest
- measuring the variables of interest

In addition, individual researchers generally lack the knowledge, tools, resources and the time to develop the models and environments that are needed, set up the number of runs required, and/or undertake a rigorous analysis of the data that would be generated by the experiment(s). This results in a dearth of the kind of experiments and analyses that the Army needs to understand, design, and operate (or attack) the composite networks of interest. The experimentation ecosystem described in this report would remove or reduce these and other barriers to composite network experimentation, and thus, enable the research that is essential for progress.

3.2 Examples of Opportunities to Extend Ongoing Research

Two major Army research initiatives provide examples of research efforts that would benefit from the development of the experimentation ecosystem proposed in this report. The first of these is the Network Science Collaborative Technology

Alliance (NS CTA) and the second is the Cybersecurity Collaborative Research Alliance (CS CRA).

3.2.1 Network Science Collaborative Technology Alliance (NS CTA)

The NS CTA unites research across organizations, technical disciplines, and research areas to address the critical technical challenges posed by the complex web of interacting networks (referred to in this report as a composite network) within which the Army mission must be performed. Its purpose is to perform foundational crossdisciplinary research in network science, resulting in greatly enhanced Soldier performance and in greatly enhanced speed and precision for complex military operations.

Network science is the study of the properties, models, and theories that apply to many varieties of networks, the understanding of how different genres of networks dynamically interact and co-evolve, and the use of this understanding in the analysis, prediction, design, and control of many varieties and systems of networks. The NS CTA research program exploits intellectual synergies across network science by uniting parallel fundamental (6.1) and applied (6.2) research across the disciplines of social/cognitive, information, and communication network research. It drives the synergistic combination of these technical areas in support of missions required of today's military forces, including humanitarian support, peacekeeping, and combat. It also supports and stimulates dual-use applications of this research and technology to benefit commercial use. To support this ambitious research program, the Alliance has created shared, distributed, experimental resources throughout the Alliance as well as a distributed network science research facility, led from the ARL Network Science Research Laboratory (NSRL) in the ARL Adelphi Laboratory Center (ALC), Maryland.

The NS CTA research program for Y6/7 (2015 and 2016) is structured into 5 interdisciplinary network science related research areas or thrusts. Each of the 5 thrusts named below require expertise in social/cognitive networks, information networks, and communication networks.

1) Quality of Information for Semantically Adaptive Networks (QoI-SAN): Measure, predict, and adapt composite networks to deliver the most valuable information with dynamically changing network resources, rather than the most bits, or queries

2) Information Processing Across Networks for Decision-Making (IPAN): Information discovery, analysis, and presentation over multi-genre networks to improve effectiveness in distributed decision-making

3) Co-evolution and Dynamics of Inter-genre Networks (Co-EDIN): Foundational science for modeling, understanding, predicting, controlling,

and optimally designing co-evolving inter-genre networks, both friendly and adversarial

4) Trust, Influencing, Modeling & Enhancing Human Performance (TIME): Improving human performance in network environments, with a focus on phenomena of trust and influence

5) Science of Multi-genre Network Experimentation (Exp): The science and research practice of meaningful integrated experimentation in complex composite networks

3.2.1.1 Semantic Quality-aware Information Delivery

There are a number of lines of NS CTA research related to semantic quality-aware information delivery (Task Q5),[3] contained in the QoI-SAN thrust, that are likely to produce research findings that could benefit by taking advantage of the capabilities which are a part of the CAMPX described in this report. These include the following:

- Source Selection: Uses meta data from sources of information to determine where overlap in information exists between all given sources. Returns a subset of the sources that maximizes information coverage over a minimal number of sources.
- Retrieval Order Optimization: Factors information timeliness/expiration and cost to retrieve information to prioritize the order in which to query information sources.
- Image Optimizer: Measures the state of the communications network and requirements of a received query. Responds with a compressed or degraded image that satisfies the query while reducing total data over the network.

Each of these capabilities have the potential to improve the quality of information that is readily available to decision makers, while at the same time provide the potential to reduce or smooth out the load placed upon the communications networks. Together these could create a virtuous cycle that could significantly improve the overall performance and agility of the composite network improving both its performance and agility, where agility is determined by what happens to network performance metrics under a wide range of missions, circumstances, and conditions.

Researchers who are exploring and experimenting with these capabilities are exploring such questions as the following:

- To what extent can a photo be compressed and still provide enough information for a given task?

- How much time and computational resources does it take to compress a photo?
- Where in the network and when should compression occur?

These NS CTA research findings may be sufficient to see if they warrant further attention, but may not be enough to ascertain if it makes sense to integrate them into the information network layer of a militarily relevant composite network. Each of these individual investigations is an instance of a capability that may be useful in one situation but less useful and perhaps even counterproductive in another situation. In addition, there may be adjustments that are needed in one or more of the component networks to realize the potential of these new capabilities or to avoid adverse impacts.

The CAMPX with its more comprehensive conceptual model, experimentation environment, and data repository of previous findings can offer the researcher the data that are required to take the next steps and investigate when these capabilities make sense and when they do not. In addition, the accumulated data can provide support to assessments that can determine the nature of the adaptations that are required to "optimize" performance while minimizing adverse impacts.

For example, the performance characteristics of the capability suggested by the NS CTA research findings could be instantiated in the CAMPX environment to investigate the nature of its impact on the composite network and determine the change it would have on composite network agility, the probability of mission success averaged over the Endeavor Space developed for the CAMPX.[4] This would enable the researcher to understand the range of missions, circumstances, and conditions under which their new capability makes the biggest difference.

Perhaps more importantly, if it turns out that simply "plugging in" the new capability makes little difference, the research community can explore the changes that may need to be made (e.g., a different approach to C2 or a different information sharing policy) in order to be able to realize the benefits envisioned. Experiment 2 (Section 4.5.2) is designed for an experimentation environment that will enable researchers who are involved in, for example, Task Q5 to take their findings, instantiate them in a composite network, and see how the behaviors and performance of the component networks are affected.

Since situations change and there will not be any one-size-fits-all solution, dynamic adaptation may be required to maintain acceptable performance and manage risks. Dynamic adaptation requires rules that govern what the nature of the adaption should be and when the adaption should occur. These rules need to be dynamically informed with data. These data could include the state of component networks, the tasks being undertaken and the state of these tasks, the roles and responsibilities of individuals and organizations, and mission requirements. A composite network

CAMPX is necessary to investigate what data are needed to support smart adaptation, the required quality of these data, and the potential of smart adaptation to increase performance and agility as well as reduce risk.

3.2.1.2 Science of Multi-genre Network Experimentation Thrust

Much of the research conducted as part of the Exp thrust would be enabled by the capabilities that are a part of the composite network CAMPX described in this report. For example, the Exp focus area that seeks to understand how information propagation is influenced by both the characteristics and performance of social (C2) and communication networks would be able to build upon CAMPX by extending the design of Experiment 2. The experimentation environment at the time of the initial operational capability (IOC) comes with analysis tools that allow researchers to trace the propagation of any given piece of information. Information propagation is a function of a number of design parameters and conditions. This feature of the CAMPX IOC environment provides an opportunity to see how information propagation changes as a function of different variables. Figures 4 and 5 compare the propagation of the same piece of information: Fig. 4 with relatively high communications bandwidth and Fig. 5 with limited bandwidth.

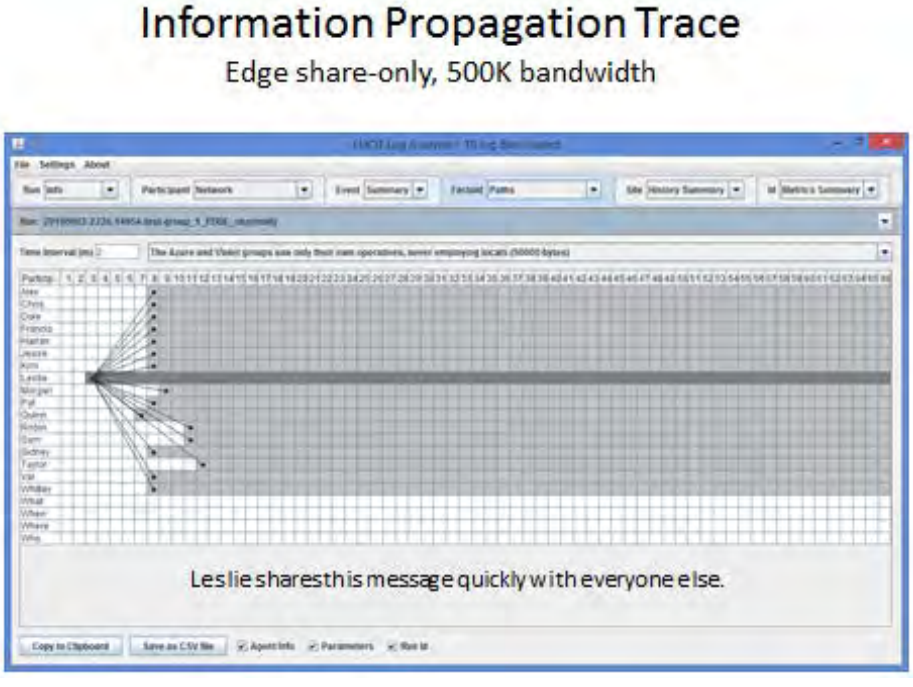

Fig. 4 Information propagation - high bandwidth

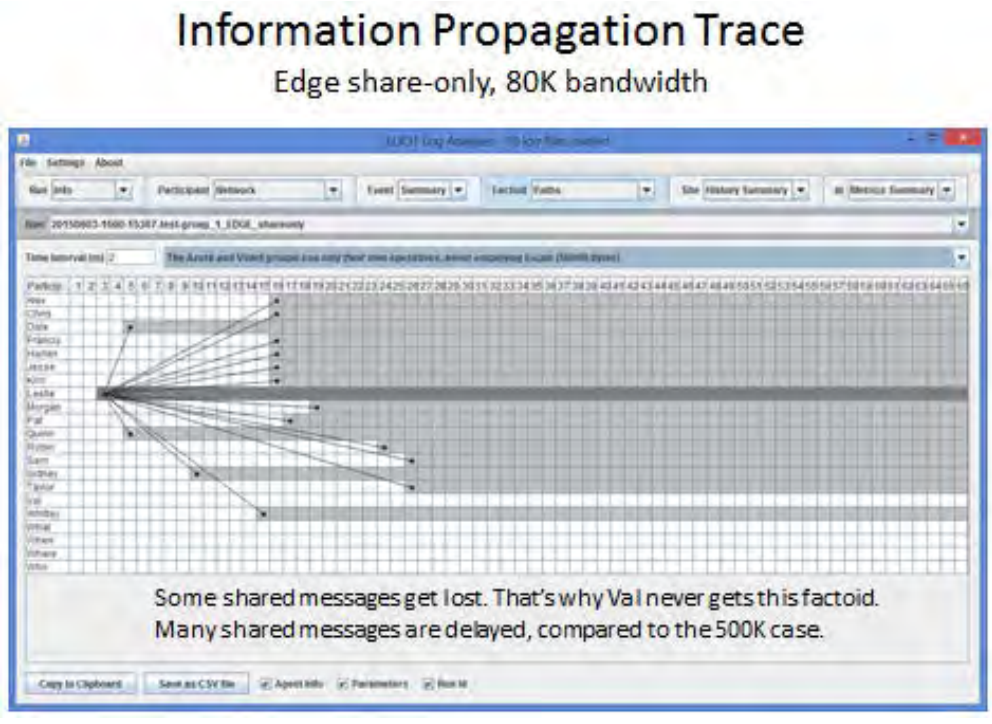

Fig. 5 Information propagation - low bandwidth

In preparation for information propagation experiments, an analysis was undertaken to understand how much information needs to be shared between and among the 4 teams in the Hierarchical C2 Approach instantiated as part of Experiment 1 as a function of the nature of the mission challenge. The results of this analysis are contained in Appendix B: The Quest for Key Information: Does C2 Approach Matter?

3.2.1.3 Information Processing Across Networks for Decision-Making

The research in this thrust will investigate social, cognitive, information and communication models to support the transformation of data into graph representations of the partially observed but mostly latent information network. Furthermore, research will investigate models to enable the information network to be accessible to the decision makers in a manner that is best matched to the cognitive abilities of these decision makers. They require extraction of information over multi-genre networks comprising of social, communications and information networks. Sometimes it is better for users to look for information that can be found on websites or in data repositories; other times it is better for users to consult subject matter experts (SMEs); and many times users should employ a hybrid approach. The decision of how to query the multi-genre network is very complex and depends on the social and cognitive states of the SME relative to the user as well as the ability of the data repository to disambiguate queries. Currently, this thrust includes research that involves human-in-the-loop network models and algorithms that will

be used to explore ways to minimize the delay for distributed decision making and improve situational understanding.

The Experimental Laboratory for the Investigation of Collaboration Information-sharing and Trust (ELICIT), featured in the IOC version of the NSRL and proposed as a common feature to bridge the Network Science and Cybersecurity research communities in Experiment 3, possesses both human-in-the-loop and agent-based capabilities that could be used to validate and explore the behaviors of models and algorithms developed in this NS CTA thrust, particularly to see how they impact mission performance in a problem-solving task under a variety of stresses and conditions.

3.2.2 Cybersecurity Collaborative Research Alliance (CS CRA) and Applied Research and Experimentation Partner (AREP) Programs

The CS CRA is a 5-year, basic research program aimed at developing a science of cyber security. The AREP program is a companion program to the CS CRA and has several goals, including development of innovative cyber experimentation technologies, and validation of the theories being developed under the CS CRA program. In particular, the AREP program features the development of a Cybersecurity Test Bed (CSTB) called CyberVAN, which is depicted in an ACS slide in Fig. 6. Briefly, CyberVAN enables applications running on virtual machines to communicate with each other across a simulated network which is implemented within a Discrete Event Simulator (DES), such as ns-3, OPNET, or QualNet. This enables very high fidelity cyber experimentation for both strategic as well as tactical military networks. In particular, wireless tactical networks can be simulated with high fidelity, using off the shelf simulation models relevant to the Army.

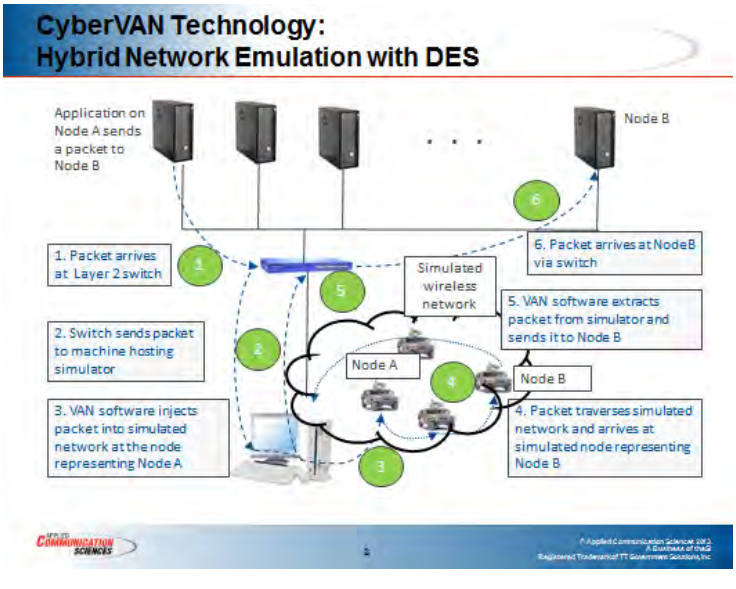

Fig. 6 Cybersecurity test bed

This test bed will be used to explore the performance and impacts of a number of cyber-defense capabilities, including those designed to counter different types of attacks (e.g., advanced persistent attacks that include various stages of intrusion, such as phishing, SQL injection, Botnets, network scanning, propagation, etc.) employing a variety of countermeasures, including behavioral changes. By implementing ELICIT agents in the CSTB, that is, by placing them on or as applications that run on the node servers, all interactions between agents and between agents and websites in ELICIT will go through the cybersecurity simulated network. Figure 7 depicts a sample network scenario in greater detail.

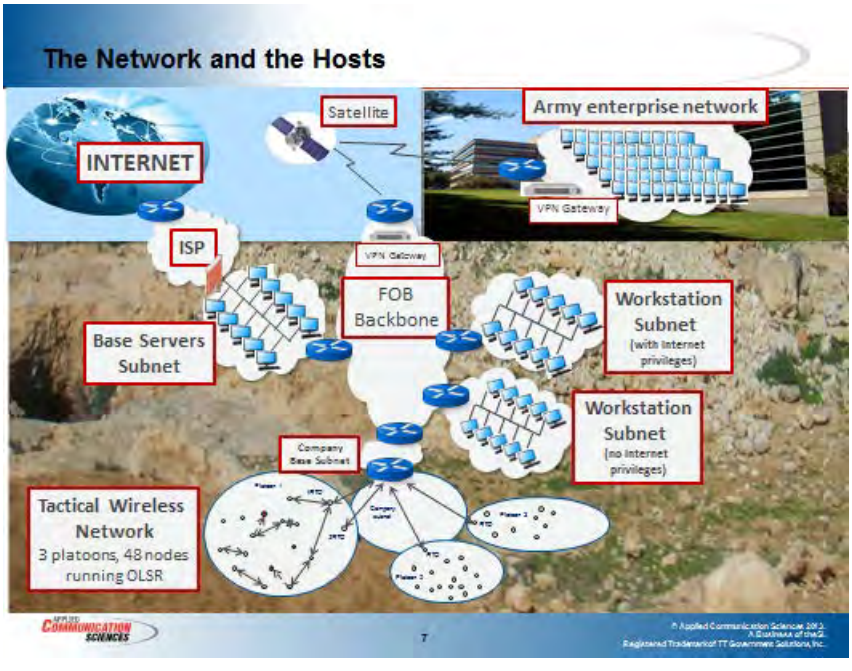

Fig. 7 Cybersecurity testbed simulated network scenario

The advantage to the CSTB is that behavioral changes can be modeled in ELICIT, as ELICIT provides a mission-level set of measures of effectiveness, efficiency, and agility. Furthermore, parallel experiments would be able to be instantiated in both the NSRL and the CSTB. This would enable researchers to observe the impacts of different cybersecurity treatments as a function of C2 Approach and information-sharing policies. The data generated from the CSTB then can be used to introduce parameters and set values for these parameters in the NSRL to reflect cyber-defense performance as a function of conditions and circumstances.

3.3 Researcher Empowerment and Productivity

The Experimentation Ecosystem not only makes it possible to investigate composite network behaviors and the consequences of its design that would otherwise not be possible, but it also empowers individual researchers enabling them to take on far more demanding research challenges then they currently are

able to attempt. Because of this, the Experimentation Ecosystem should attract a variety of researchers, thereby increasing the breadth and depth of the talent available across a range of disciplines to investigate composite network behaviors and design. Although empowered, individual researchers will nevertheless find it necessary to enlist the help of others with complementary skills and expertise and to work as part of an interdisciplinary team in order to tackle some composite network issues. Thus, the ecosystem facilitates this necessary interdisciplinary collaboration and helps bring needed expertise to bear on research questions that cut across academic disciplines.

Not only does the Ecosystem empower researchers by enabling them individually and in teams to undertake more challenging research projects, but it enables them to increase the quality of the research while reducing the time and effort required. This is accomplished by providing access to tools that allow more rapid and sophisticated analysis of data and by eliminating duplicative investments in research. Thus, a research ecosystem enables the community as a whole to better leverage data and findings. This Experimentation Ecosystem accelerates knowledge accumulation and progress and will enable the Army to field more effective, efficient, and agile composite networks sooner than would otherwise be accomplished.

4. Composite Network CAMPX

This section begins with a discussion of military relevance that provides the overall context for the campaign and a statement of the goals of such a campaign.

4.1 Military Relevance

While there is considerable merit in improving our understanding of network behavior in general, the networks necessary to support Army operations have a set of characteristics and operate in environments that distinguish them from networks in the abstract. Thus, while Army research efforts include investigations of domain-free networks, they also need to understand the specific characteristics and constraints associated with the networks that support Army operations that makes them special cases, and how these factors impact network behaviors and the implications for the design of these networks.

The Army Composite Network (collection of technical/social/cognitive networks) must enable commanders and their staffs to accomplish the variety of C2 functions and other mission-essential tasks. Thus, Army networks are purposeful and constrained in ways that differ from many of the networks that exist in society and have been studied for a number of years in the network science community.

While cybersecurity is a consideration that is common these days to networks of all types, Army networks operate in a highly contested environment and are subjected to a variety of physical, electromagnetic, and cyber-attacks. Another consideration is the variety of entities which are interconnected by Army networks including individuals, organizations, systems, and entities that have varying degrees of autonomy.

Thus, in addition to developing a better understanding of networks in general, we also need to focus adequate attention on the complex composite networks employed by the Army. By doing so, we will learn what to observe, how to measure it, what affects Army network performance and military outcomes and why it does. Only then will we be in a position to develop an integrated design of the Army Composite Network.

Increased understanding enables us to do a better job of predicting outcomes as a function of circumstances and conditions. This increased ability to predict offers an opportunity to influence/control outcomes by appropriate network design and management of composite network components. This, in turn, improves our ability to exert influence and control the behavior of mission-critical composite networks and, by doing so, we can increase network agility and the probability of maintaining acceptable levels of network performance under a variety of circumstances. For these reasons, the CAMPX envisioned here focuses its attention on militarily relevant network research.

4.2 Goals

CAMPX goals include a set of achievements in each of the following areas.

- Research

  Develop a basic understanding of the critical interdependencies that exist between and among the communications, information, and social networks that constitute mission-focused composite networks and their implications for network behaviors and performance, approaches to C2, and mission effectiveness and force agility.

  Develop an approach to integrated design of composite networks that result in improved mission performance and agility.

- Programmatic

  Provide a framework that can integrate, synchronize, and synthesize ongoing and planned network-related research and experimentation being pursued within ARL and within the NS CTA, CS CRA, and related research efforts both within DOD and external to DOD.

- Community

  Facilitate and enable the interdisciplinary collaborations, experiments, and analyses necessary for progress.

- Methodological

  Demonstrate the feasibility and value of moving from individual experiments to campaigns of experiments.

4.3 Conceptual Model

The conceptual model for a CAMPX that seeks to understand and shape the behaviors of militarily relevant composite networks needs to include, at a minimum, the following models and the relationships between and among the variables contained in these models:

- Endeavor Space Model
- Single-Genre Network Models
- Cybersecurity Network Model
- Composite (multi-genre) Network Model
- Composite Network Value Chain

4.3.1 Endeavor Space

An Endeavor Space is a multi-dimensional space that includes the set of conditions and circumstances that could impact composite network and mission performance. Endeavor Space dimensions are associated with specific characteristics of the mission, the environment, and the states of the relevant entities and actors. Each region of this space provides a specific mission context and specifies the conditions of interest that can impact network behaviors, measures of performance (MoPs) and measures of effectiveness (MoEs). These conditions and circumstances provide inputs to the other models (e.g., single-genre network models, cybersecurity model). By using these inputs as their initial conditions (and as they are dynamically updated) these models can generate the metrics needed to determine the overall performance and agility of the composite network and when compared to mission requirements, determine (likelihood of) mission success or failure. Figure 8 depicts the initial formulation of a 6-dimensional Endeavor Space.

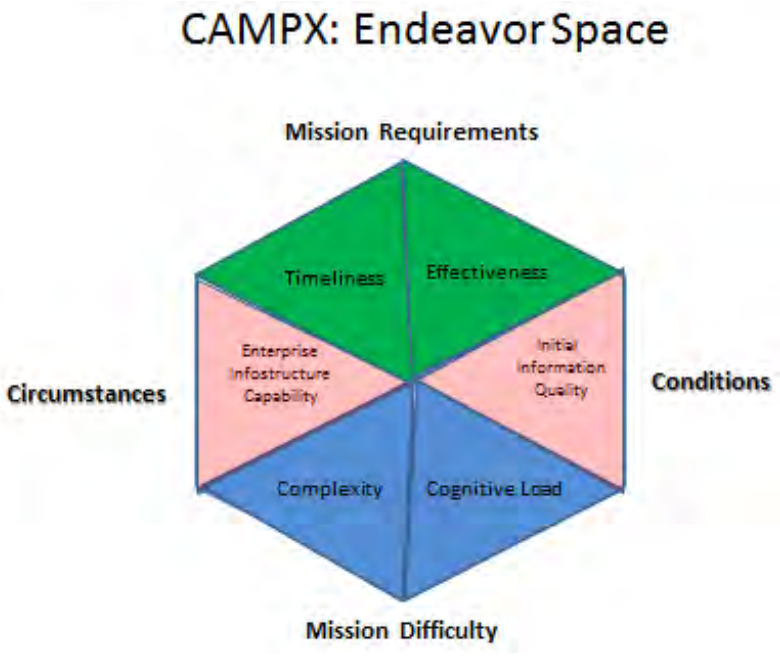

Fig. 8 CAMPX Endeavor Space

Four of the dimensions of the Endeavor Space are devoted to the nature of the missions, including 2 dimensions that are concerned with mission requirements (timelineess and effectiveness) and 2 dimensions that are devoted to mission difficulty (complexity and cognitive load). In addition, 2 dimensions focus on the circumstances and conditions under which a mission is undertaken (infostructure capability[5] and initial information quality). The difficulty of the mission and the circumstances under which a mission is undertaken can be expected to impact network performance or quality of service while mission requirements allow us to translate given levels of performance into mission outcome related metrics.

4.3.2 Single-Genre Network Model

A single-genre network model links a set of network design parameters (e.g., a mobile communications network) to network behaviors and performance dynamics under specified circumstances and conditions (regions of the endeavor space). Figure 9 is a depiction of a single-genre network model. The outputs of this model are a set of values for the network performance metrics (e.g., for a communications network, and the probability of correct message receipt as a function of time) for selected regions of the Endeavor Space.

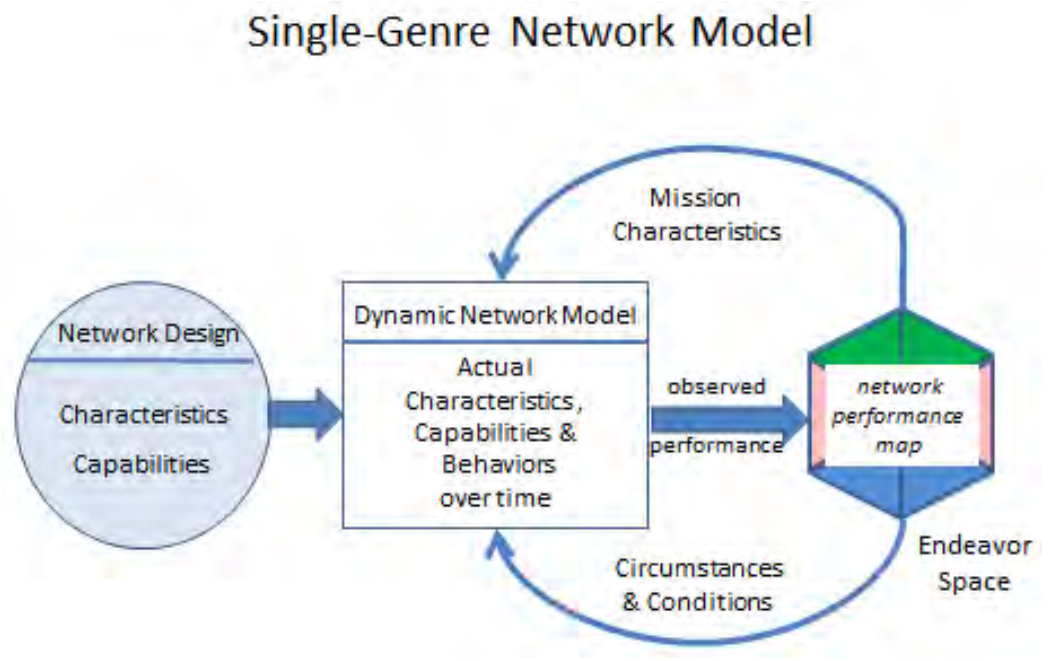

Fig. 9 Single-genre network model

4.3.3 Cybersecurity Model

The operating environments of interest will be contested and adversaries will routinely seek to deny and/or degrade our ability to operate at will, utilizing a variety of means. Both physical and cyberattacks on our networks will be commonplace. The term "cybersecurity" is used here to refer to the range of measures and actions we take to prevent our networks from being destroyed, damaged, degraded, or compromised in some manner. Ultimately the impact that cybersecurity has upon network behaviors, performance, and agility are a result of both our own and adversary defensive and offensive capabilities and actions. These need to be represented in the various components of the CAMPX conceptual model.

In addition to the ability to represent various states of network dysfunction and performance in the components of the CAMPX conceptual model and their related impacts, these models need to account for multiple perceptions. These perceptions include the nature of the threat and the impacts that may affect network design choices and network operating protocols that are needed to implement both passive and active defensive measures in order to manage these perceived risks.

Defensive measures incur a variety of costs, as they not only consume resources that could be used for other purposes, but they can constrain network behaviors. In the absence of an attack, defensive measures adversely impact network performance (individual networks and composite network) with the arguable benefit that their presence may have deterred or altered some attacks. In the presence of an attack, they serve to prevent or mitigate damage that would have

otherwise occurred. As a result of these defensive measures, network performance is better than it would have otherwise been under selected conditions and circumstances. In situations when network performance would have been reduced to unacceptable levels and when the defensive measures result in network performance remaining or regaining acceptable levels, agility is increased, and mission risk is reduced.

Other factors that should be incorporated into the CAMPX conceptual model (the set of included models) include perceptions regarding adversary capabilities that influence decisions, if and when to employ offensive cyber operations. These offensive operations incur costs and invite a range of responses which have impacts that are a function of defensive capabilities and if, when, and how they are employed. The response to the new network state that is created and its subsequent impacts on behaviors and performance depend upon a host of factors which also need to be considered.

Figure 10 depicts how cybersecurity considerations need to be incorporated into the single-genre network models.

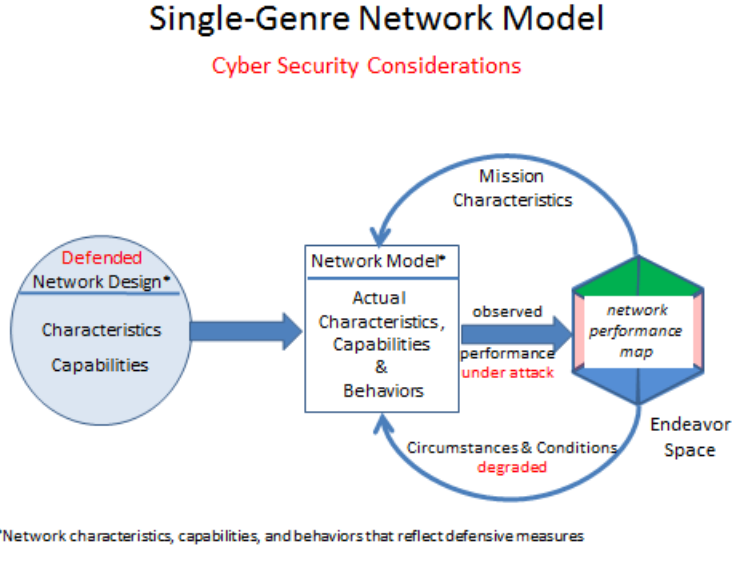

Fig. 10 Incorporating cybersecurity into a single-genre network model

Among the changes that need to be made to a network model to reflect cybersecurity considerations are 1) adding cybersecurity design-related parameters and specifying their relationships to other design parameters; 2) specifying the relationships between and among the cybersecurity related design parameters and the variables that affect network behaviors; and 3) incorporating the impacts that reflect the circumstances and conditions that represent the results of a cyberattack into the network model.

In addition to the cybersecurity-related changes that need to be made to the network models, changes are also needed to the Endeavor Space dimensions. These changes need to reflect cybersecurity-related circumstances and conditions. Figure 11 identifies those considerations. To appropriately represent the situations, we need to be consider in an analysis of network agility, the Endeavor Space must contain regions that 1) map to the cybersecurity related capabilities of the infostructure; 2) represent various levels of information quality that can result from a successful cyberattack, given the employment of specific defensive measures; and 3) map the effects that can result from a degraded infostructure and information quality on the cognitive loads placed on individuals and on the complexity of the tasks that need to be accomplished.

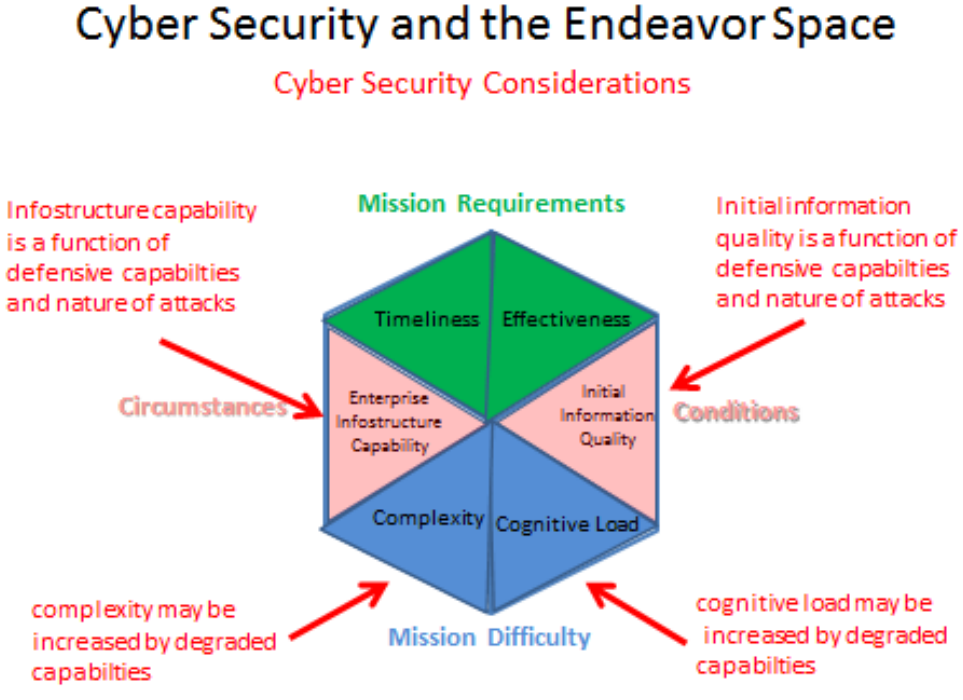

Fig. 11 Incorporating cybersecurity considerations into the Endeavor Space

4.3.4 Composite Network Model

The Composite Network Model consists of the various single-genre network models that incorporate cybersecurity considerations, the model of the endeavor space, and the relationships between and among the variables contained in these models as depicted in Fig. 12.

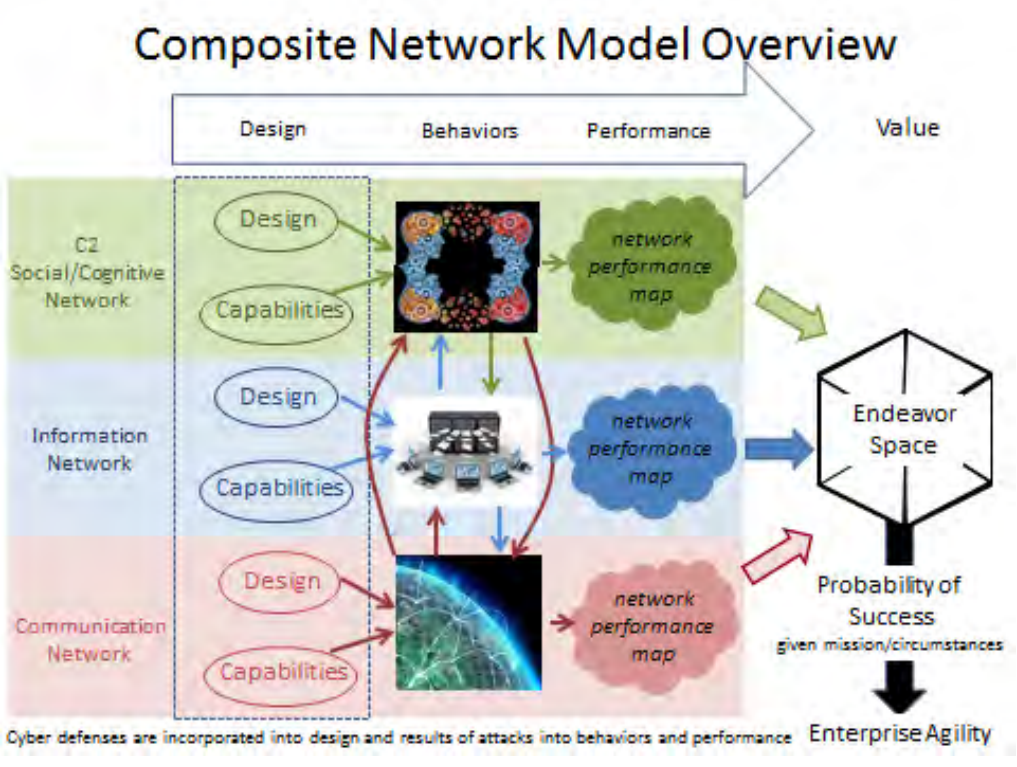

Fig. 12 Composite Network Model overview

4.3.5 Composite Network Value Chain

The ultimate goal is to arrive at an integrated design of a composite network, one that balances all performance tradeoffs in a way as to achieve acceptable levels of performance for missions and circumstances of interest. To accomplish this aim, one needs to specify an end-to-end value chain that links the individual network design parameters to mission performance for the different regions of the Endeavor Space. Such a value chain is depicted in Fig. 13.

This value chain relates network design parameters to quality metrics. These, in turn, when measured for different points in an Endeavor Space, result in a measure of agility. However, design parameters, network quality and agility are not the only measures of interest to researchers, experimenters, analysts, and operators. There are a host of other intervening values that affect the relationships between design, quality, and agility. The North Atlantic Treaty Organization (NATO) C2 Conceptual Reference Model identifies a number of these.

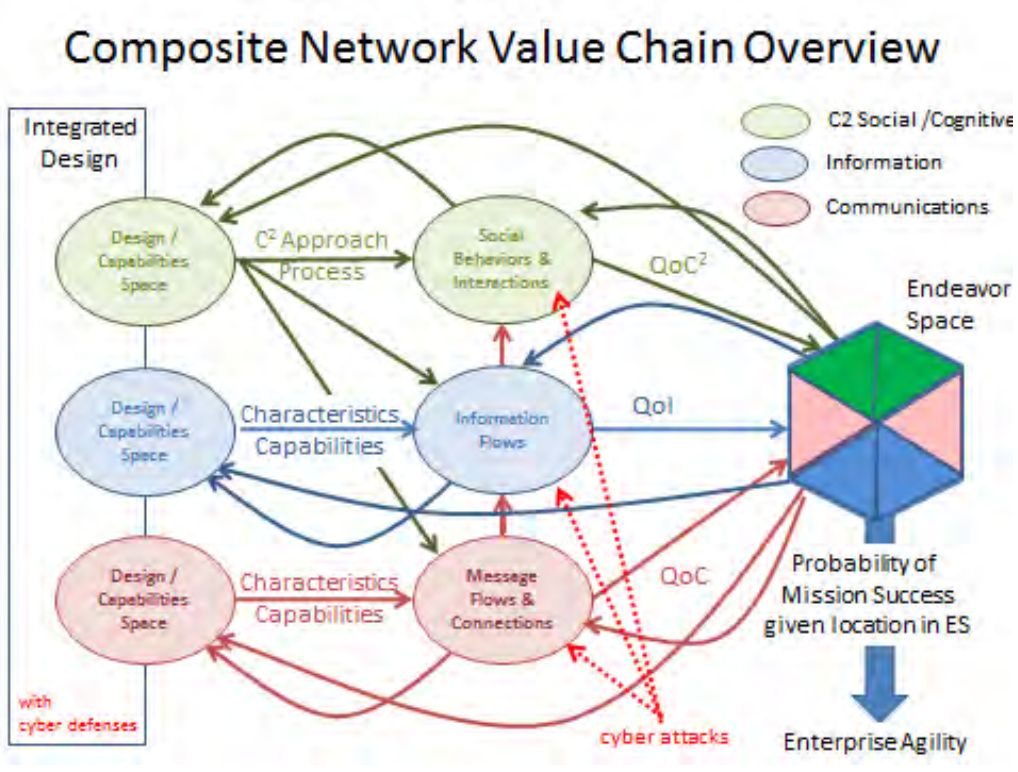

Fig. 13 Composite network value chain

4.4 Hypotheses and Metrics

The experiments that will be undertaken as part of the effort to understand, and ultimately, influence composite network behaviors will be conceived and designed to address a set of hypotheses suggested by the composite network conceptual model. This hypothesis testing activity 1) seeks empirical support for key aspects of the conceptual model that have been specified; 2) serves to establish or fine tune relationship parameters; and 3) fills in areas of the model that need more specificity. Designing experiments to test hypotheses requires the definition of a set of metrics. Conducting these experiments involves instantiating specific values or ranges of values for the independent variables and being able to observe the resulting values associated with the dependent variables. This section discusses a set of first-order hypotheses related to composite networks and the metrics associated with them.

4.4.1 Network Hypotheses

Composite networks are collections of interdependent, interacting networks. In the composite networks of interest here, this collection consists of networks of different genres. Given the limited state of our understanding of individual networks, the composite network CAMPX will need to consider experiments that explore hypotheses that pertain to both specific single-genre networks as well as those that explore the interdependencies and relationships between and among networks of

different genres. The results of these experiments will enable us to better understand possible design tradeoffs between and among the characteristics and performance of the individual networks and to develop and test integrated composite network designs.

Network hypotheses consist of statements about the relationships between and among the characteristics and performance of individual networks and composite network characteristics and performance and/or between composite network performance and mission-related metrics. The following are a set of hypotheses that address the nature of a composite network:

- Enterprise effectiveness (mission success under a given set of conditions and circumstances) is a function of the measures of quality (Q) associated with each of the network genres.
- The Q delivered by one network can compensate for a lack of quality delivered by a related network thus maintaining a given level of task effectiveness.
- Composite network Q and agility can be improved by building in the ability to sense the condition/performance of individual networks and context-aware behaviors provided that appropriate options are available and properly employed.[6]
- The agility of one network can compensate, at least to some degree, for a lack of agility in a related network.
- Composite network agility is a function of the agility of each of the networks.
- Cyber vulnerabilities in one network cannot be totally offset by a lack of vulnerabilities in related networks.

Individual network hypotheses consist of statements about the relationships between and among network design parameters and performance of individual networks under a variety of conditions (e.g., load). The following are a set of hypotheses that address the nature of an individual network:

- Network Q are a function of network design, network capabilities, and the prevailing circumstances and conditions.
- The agility of a network (ability to deliver acceptable levels of their Q over an Endeavor Space) is a function of network design and operation.
- Network Q and agility can be improved by more effective cyber capabilities and/or by building in self-aware behaviors provided that appropriate options are available and properly employed.

Both sets of hypotheses identified above refer to network Q and agility are generic as they refer to unspecified single-genre networks. To test these hypotheses, more specificity is required regarding how the quality of each of the networks is to be measured, what constitutes acceptable performance for each of these networks, and the dimensionality of the endeavor spaces that will be used to determine network agility.

Each type of network exists to provide a set of services that enable an enterprise to carry out its missions. The goals of each of the single-genre networks and of cybersecurity, specific hypotheses of interest, and the associated metrics that will be employed in experiments and analyses are discussed below.

4.4.2 Information Network: Goal, Hypotheses, and Metrics

The goal of an information network is to assure the delivery of information of sufficient quality to meet the mission needs of 1 or more cognitive/social networks (e.g., C2, task) over the range of mission requirements, circumstances, and conditions. Thus, the Q of an information network is the quality of information (QoI) delivered by the network as a function of time and region of the endeavor space.

A major component of the network science research sponsored by the Army is focused on improving the quality of information that is available to support decision making on the battlefield. One of the research objectives is to increase the intelligence of information network agents and processes. This includes building information networks that are aware of themselves (self-aware) and their environment (context aware). This is because self-aware networks, those that are aware of their current performance and capability limitations, could be programmed to behave differently, given changes in their capabilities and capacities (e.g., degraded modes of operations). The following 2 related hypotheses are based upon this research objective:

- Information networks can be made to be both self-aware (the state of their capabilities and capacity) and context aware, that is, aware of the external conditions that include the state of other networks and mission-related conditions.
- Increased self and context or situation awareness can be used to dynamically modify information-related network behaviors and improve information network QoI and agility.

QoI is measured by 2 sets of metrics. The first set consists of “absolute” measures, that is, objective measures that are independent of the mission/scenario. The second set consists of “fitness-for-use” measures, measures that look at the quality of information in the context of the task at hand. For example, the actual time that has

elapsed between an observation and the time it is made available to an individual is an absolute measure while the timeliness of this information, that is, whether or not the time delay is acceptable for the task at hand is a relative measure. Fitness for use measures are used to determine what are acceptable levels of performance.

Figure 14 provides the principal measures from each set that are incorporated into the conceptual model and will be employed in the experiments. These measures are not independent of one another and the nature of the relationships that exist should be part and parcel of this CAMPX. The question of how one can combine these many dimensions of information network quality into a single measure is often raised. However, developing a 1-dimensional measure is problematic because the relative importance of each of these "dimensions" of quality is a function of the mission, circumstances, and conditions. These will be reflected in behaviors and outcomes observable in both the C2 network and the mission.

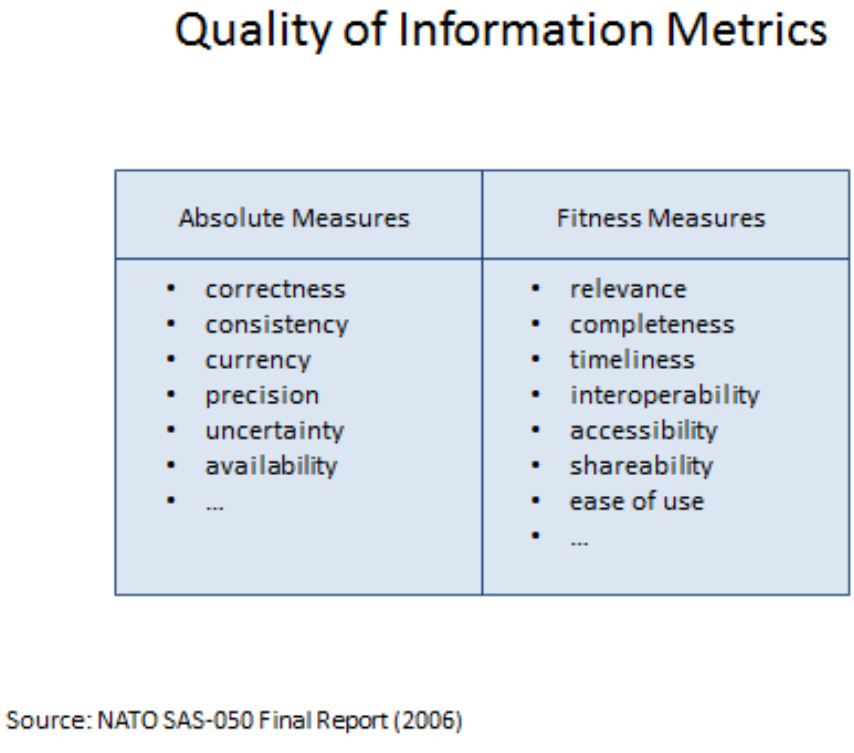

Fig. 14 QoI metrics

Measuring information quality consists of making observations (recording values in instrumented environments) at various points in time. As a result, information quality measures can be averaged over a period, expressed as a function of time, or in terms of the probability of success (the probability the variable in question is within an acceptable range over some period of time).

Each observation, recording, or measurement takes place in a specific mission context and set of circumstances. Thus, the set of measures used to determine an

information network's QoI can reflect the ability of the network to maintain an acceptable level of performance, in other words, the network's agility, by recording their value as a function of the mission and circumstances. The set of these values can be mapped onto the Endeavor Space and then compared to the mission requirements map (the QoI performance requirements for each mission/ circumstance) to create an information network effectiveness map. The information network effectiveness map is used to calculate network agility and compare the agility of various networks. Figure 15 depicts the process by which measures of network QoI performance are transformed into an information network effectiveness map.

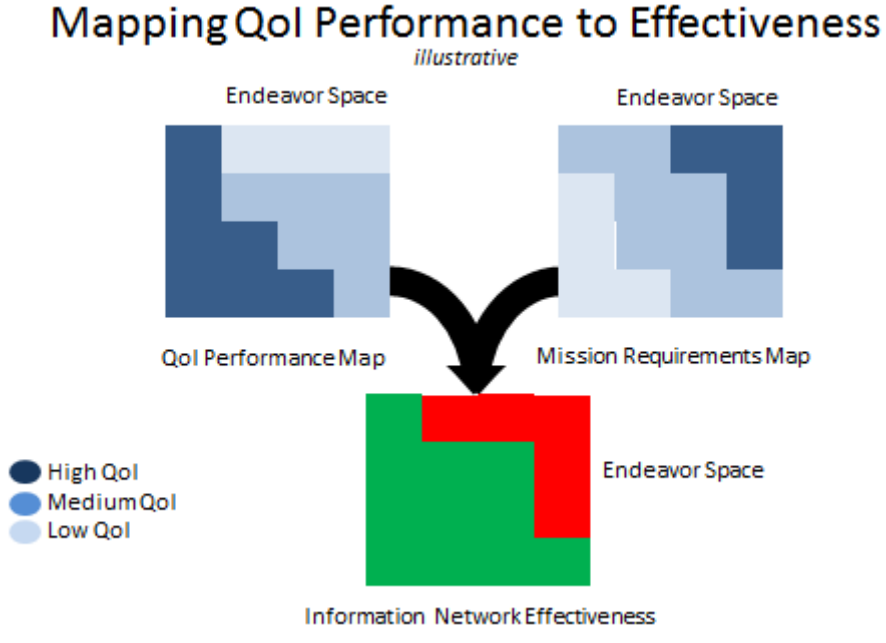

Fig. 15 Mapping QoI performance into effectiveness

4.4.3 Communication Network Goal, Hypotheses, and Metrics

The goal of a communication network is to enable the interactions and data flows necessary to meet information quality requirements and the mission needs of 1 or more cognitive/social networks (e.g., C2, task) over the range of mission requirements, circumstances, and conditions. Thus, the Q of a communication network is the quality of communications (QoC) delivered by the network as a function of time and region of the Endeavor Space.

A major component of the network science research sponsored by the Army is focused on enabling necessary connectivity and message throughput despite an austere and contested communications environment. As is the case for information networks, efforts aimed at making communication networks more self and context aware are underway.

The following 2 related hypotheses are based upon this research objective:

- Communications networks can be made to be both self-aware (the state of their capabilities and capacity) and context aware, that is, aware of the external conditions which include the state of other networks and mission-related conditions.
- Increased self and context or situation awareness can be used to dynamically modify communications-related network behaviors and improve QoC and agility.

As is the case with QoI, QoC is measured by 2 sets of metrics. The first set consists of "absolute" measures, that is, objective measures that are independent of the mission/scenario. The second set consists of "fitness-for-use" measures, which look at the quality of communications in the context of the task at hand. For example, the actual time that has elapsed between the first attempt to "transmit" a message and the time(s) it is made available to its intended recipients is an absolute measure while the timeliness of this communications refers to whether the delay incurred is acceptable for the task at hand is a relative measure.

Measuring the quality of communications consists of making observations (or recording values in instrumented environments) at various points in time. As a result, QoC measures can be averaged over a period, expressed as a function of time, or in terms of the probability of success (the probability the variable in question is within an acceptable range over some period of time).

The probability of correct message[7] receipt as a function of time, PCMR(t), is an absolute measure of communications network performance. A fitness for use measure would be what fraction of messages were delivered in a timely manner. This can be calculated from PCMR(t) and mission timeliness requirements and represents communications network latency relative to requirements. However, for these experiments, we need to measure how PCMR(t) is affected by a variety of network design parameters, conditions, and circumstances. Does the curve shift to the right or left, does the shape of the curve change? These parameters of interest include network topology and connectivity, protocols, load on the network, and damage to the network.

Each observation, recording, or measurement takes place in a specific mission context and set of circumstances. Thus, the set of measures used to determine an information network's QoC can, by recording their value as a function of the mission and circumstances, create a communication network effectiveness map using the same process described for information networks. This map can be used to calculate communication network agility and compare the agility of various communication networks.

4.4.4 C2 Social/Cognitive Network: Goal, Hypotheses, and Metrics

Army C2 social/cognitive networks have 2 major interrelated purposes. First, to accomplish the functions associated with C2, and second, to accomplish mission essential tasks in pursuit of mission objectives. In order words, Army "social networks" are purposeful and are organized and operated in accordance with the selected approach to C2. The goal of Army C2 social networks is to assure the development of the shared awareness necessary to synchronize effects in order to satisfy mission requirements over the regions of the Endeavor Space that are of interest.

That having been said, Army social networks nodes (humans and/or automated decision maker agents) often need to interact with counterparts in other social networks, both military and civilian, to assure that Army actions are appropriately supported or supporting a larger joint, combined, coalition, or collective enterprise.

The following 2 related hypotheses are based upon this research objective:

- C2 social/cognitive networks (commanders and other nodes) can be made to be both self-aware (the state of their capabilities and capacity) and context aware, that is, aware of the external conditions that include the state of other networks and mission-related conditions.
- Increased self, context, or situation awareness can be used to dynamically modify C2 social/cognitive network behaviors (maneuvering in the C2 approach space) and, as a result, improve quality of C2 (QoC2) and agility.

Commanders, by virtue of their selection of a C2 approach, establish the constraints and conditions that largely determine the behaviors of Army social networks as well as impact the behaviors of the inter-dependent information and communications networks that are part of the composite network

The CAMPX C2 social/cognitive network design space is the set of feasible C2 approach options. These options correspond to different regions of the C2 approach space. The C2 approach space, with the set of NATO network-enabled C2 approach options, is depicted in Fig. 16.

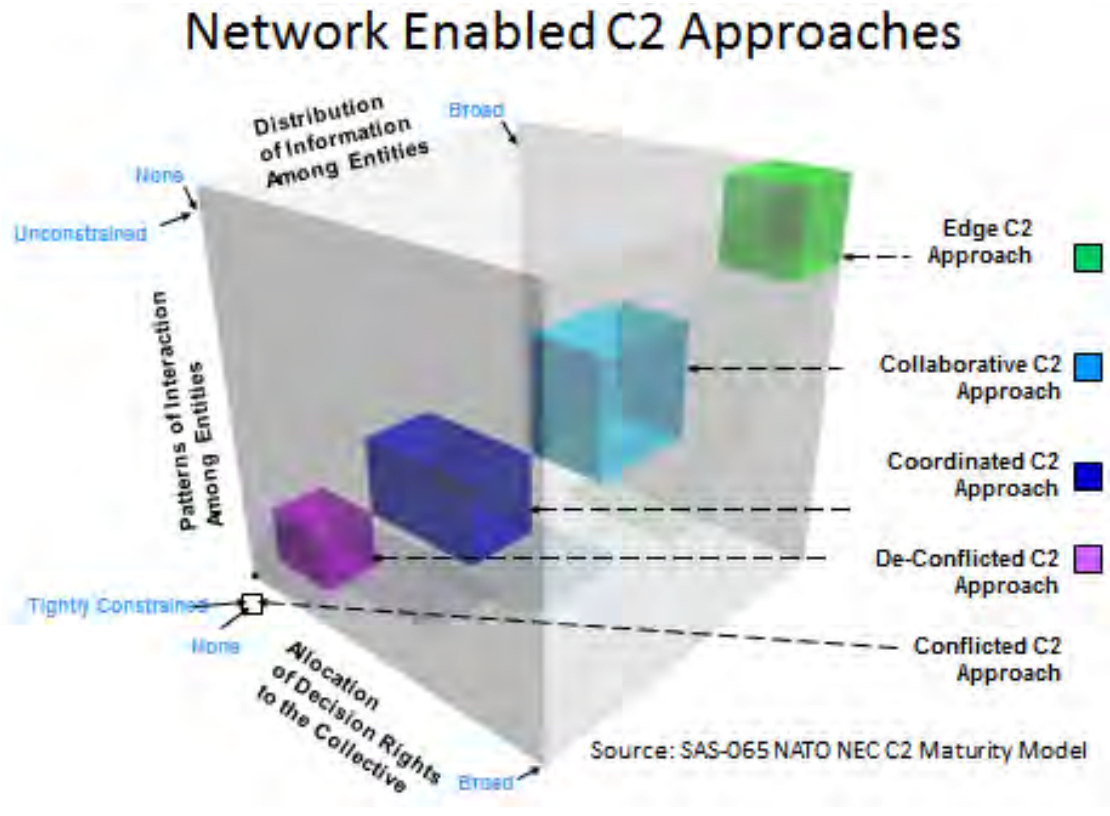

Fig. 16 Network-enabled C2 approaches

4.4.5 Network Cybersecurity: Goal, Hypotheses, and Metrics

Cybersecurity needs to be integral to the design and operations of a composite network. The goal of network cybersecurity is to assure mission accomplishment despite cyber or other attacks on 1 or more of the networks. The design challenge is to balance cyber-defense capabilities across a set of networks such that it maximizes mission success and minimizes costs.

Two cybersecurity-related CAMPX-level hypotheses that will be investigated as part of the campaign of experimentation are the following:

- A balanced, integrated security design minimizes the adverse impacts of cyber attacks
- The agility of one or more networks compensates for a lack of defensive capability in other networks.

While ultimately the quality of cybersecurity (QoCS) is measured by the ability of the single-genre networks to function acceptably (and thus ensure the appropriate functioning of the composite network) the performance of cybersecurity can be measured by resilience metrics. Resilience metrics measure the ability to regain acceptable levels of performance as a function of time following an attack that damages a network. In the case of interdependent networks, the effects of damage

propagate and thus a measure of resilience needs to reflect the "repair" and/or mitigation of the damage and restoration of service.

4.4.6 Integrated Composite Network Design

The nature of the interactions between and among the single-genre networks and cybersecurity measures that make up a composite network create interdependencies and result in a level of complexity such that the traditional design approaches employed for the individual networks are unlikely to result in "optimal" composite network performance and effectiveness. This is because there will need to be tradeoffs involving less than "optimal" performance of individual networks in the interests of overall performance and effectiveness. Therefore, an integrated design approach is needed for composite networks, an approach that takes into consideration the possible tradeoffs between and among individual network performance and effectiveness. Thus, the set of composite network design parameters contains all of the design parameters for the individual networks and cybersecurity.

The goal of composite network design is to balance capabilities across set of networks such that it maximizes the probability of mission success (agility).

A hypothesis central to this composite network design goal is that an integrated composite network design will result in acceptable composite network performance even if there are performance shortfalls in 1 or more of its networks. A related hypothesis is that the agility of 1 or more networks can compensate for a lack of agility in other networks and ensure acceptable composite network performance.

Figure 17 is a graphical depiction of the inter-relationships between individual network agility and overall composite network or enterprise agility. This depiction does not take into consideration any agility-related compensation effects; that is, when either the performance of one network or adapted behaviors compensation for a lack of performance in another network. Figure 18 takes into consideration the ability of the C2 network to adapt its behaviors in situations where the communication and information networks fail to meet mission requirements.

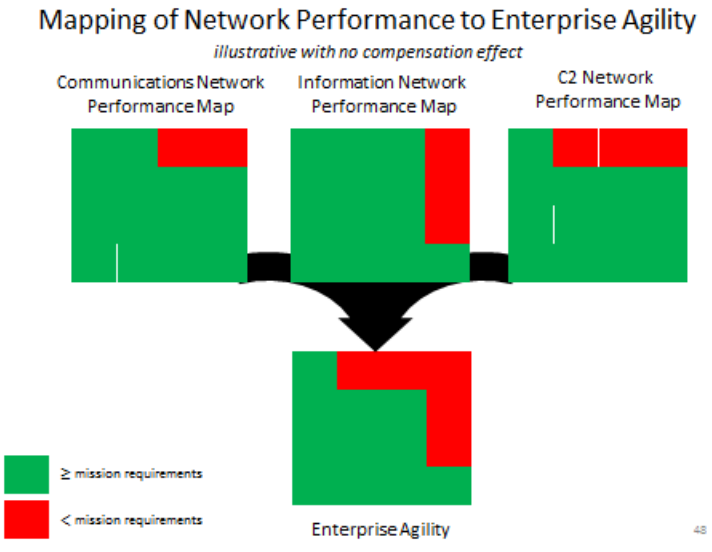

Fig. 17 Mapping network performance to composite network agility without compensation effects

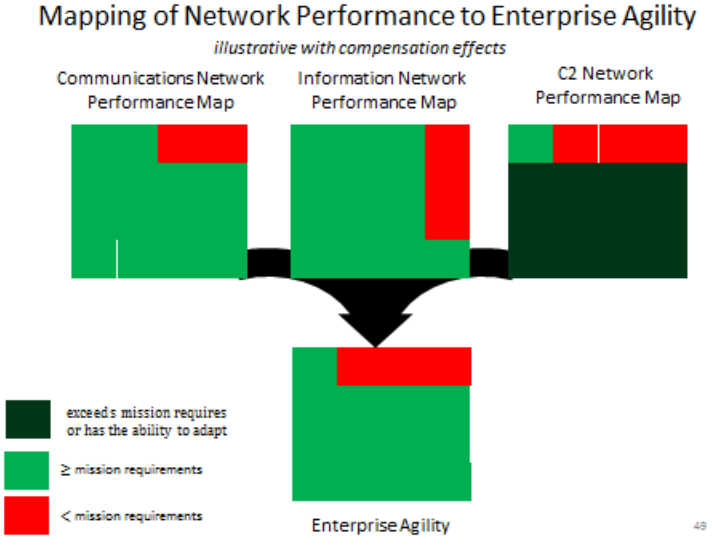

Fig. 18 Mapping of network performance to enterprise agility with compensation effects

Of course, composite networks are there to support multiple missions. While this report focuses on experiments that involve a single mission, extending them to consider simultaneous missions can be accomplished using the same basic approach and metrics. The limiting factor is the capability of the experimentation environment to support simultaneous mission simulations. Should the environment not be able to support multiple simultaneous missions, using an approach that generates network traffic to account for other concurrent missions is an alternative.

4.5 Initial Experiments

As previously discussed, adequate exploration of any of these hypotheses will require multiple experiments, each with a relatively large number of runs. The nature of the first few rounds of experiments in a CAMPX to explore composite networks behaviors will, of necessity, be constrained by the characteristics and capabilities of the available experimental environments. In this Section, 3 initial experiments are discussed. Their selection was based upon their potential to contribute to improving our understanding of composite networks, a desire to gain experience with experimenting with multi-genre composite networks, and the capabilities of the existing experimentation infrastructure. The first experiment was constrained by the capabilities of existing experimentation venues while the second and third were designed to take advantage of selected enhancements in these capabilities that could be realized in the next 2 years.

An experimental proposition or hypothesis is either taken directly from an explicitly articulated conceptual model or implies 1 or more relationships in a conceptual model. These relationships are normally qualified, that is, the existence or form of a relationship between or among a set of variables is conditional upon the value(s) of 1 or more variables. An experimental proposition or hypothesis shapes the design and conduct of an experiment by determining the nature of the data that needs to be collected. For this CAMPX, critical data include the behaviors and outcomes and the circumstances and conditions. Metrics specify how the values of each of the variables will be observed and measured.

The formulation of an experiment requires the specification of the proposition or hypothesis(es) to be investigated, the metrics necessary to describe and characterize observed behaviors and outcomes, the experiment design, and the environment.

The design of the experiment also takes its “direction” from the experimental proposition or hypothesis. The design of an experiment consists of the identification of the controllable variables and the values that they will take on for both the treatments and the conditions and circumstances of interest. The treatments correspond to specify network characteristics and intended performance targets while the conditions and circumstances of interest specify the regions of the Endeavor Space that will be sampled.

The experimental design determines the requirements for the experimentation venue or environment. The environment creates the “reality” in which the behaviors of interest and outcomes take place and are documented. The capabilities and characteristics of the environment determine how entities and networks are represented. In particular, the instrumentation capabilities determine the data that can be collected. Some venues/environments have built in data processing and analysis tools.

Three experiments are discussed to varying levels of specificity in the sections that follow. Experiment 1 is specified at a level of detail sufficient to undertake it in the NSRL. An initial design for Experiment 2 is provided in anticipation of enhancements to the NSRL's existing capabilities. The experiment is described at a level of detail sufficient to 1) serve as a guide to the specification and development of a set of enhancements that would allow the NSRL to support more rigorous composite network experimentation, and 2) provide the outlines of an experimental design concept that can be completed when the specifications of the enhancements have been finalized. A concept for a third experiment (Experiment 3) is provided; one that requires some integration of the NSRL IOC+1 capabilities and a planned cybersecurity test bed to be developed under ARL's CS CRA (IOC+2).

4.5.1 Design of Experiment 1

Experiment 1 is intended to be the first in a series of experiments that will collectively constitute a multi-threaded CAMPX designed to explore issues related to the performance of composite networks; specifically issues related to the interdependencies between and among its component networks (communications, information, C2 – social/cognitive) and its cybersecurity capabilities.

4.5.1.1 Experiment 1 Goal

The goal of Experiment 1 is to provide a "proof of concept" and a migration path for subsequent experiments and analyses that will strive for greater granularity and fidelity. Experiment 1 is constrained by the capabilities that are available in the IOC version of the NSRL Experimentation Infrastructure, this experiment involves assembling existing components. To accomplish this goal, Experiment 1 needs to do the following:

- involve the accomplishment of a military task
- represent dynamic network interdependencies that involve 2 of the 3 genres (social and communications)
- represent cybersecurity impacts as a proxy for cybersecurity capabilities
- observe/instrument network quality metrics
- measure task accomplishment (enterprise value)
- establish a baseline for subsequent experiments
- provide "hooks" to explore the impacts of proposed improvements to network capabilities (e.g., context aware behaviors)

One of the CAMPX milestones that will be accomplished by conducting this experiment will be the creation of an extendable experimentation environment that

provides the context necessary to link design parameters for 2 single-genre networks to network performance on an individual basis, as well as to the performance of a 2-genre composite network.

4.5.1.2 Experiment 1 Propositions and Hypotheses

Experiment 1 is designed to explore both single-genre and composite network hypotheses.

For the composite network formed by communications between these 2 networks, the data provided by Experiment 1 will be used to determine the extent to which there is empirical support for the following hypotheses:

- Enterprise (task) effectiveness (success) is a function of the measures of quality associated with the network genres.
    - Mission success is a function of QoC.
    - Mission success is a function of QoC2.
- The quality delivered by 1 network can compensate for a lack of quality delivered by an interdependent network thus maintaining a given level of task effectiveness.
    - An increase in QoC can offset a decrease in QoC2 and thus result in a probability of mission success that is equal to or greater than would have occurred otherwise.
    - An increase in QoC2 can offset a decrease in QoC and thus result in a probability of mission success that is equal to or greater than would have occurred otherwise.
- The agility of one network can compensate for a lack of agility (ability to deliver acceptable levels of quality over an Endeavor Space) in a related network.
    - An increase in communication network agility can offset a reduction in the C2-social network agility and thus result in a probability of mission success than would have occurred otherwise.
    - An increase in C2-social network agility can offset a reduction in communication network agility and thus result in a probability of mission success than would have occurred otherwise.
- Composite network agility is a function of the agility of each of its component networks.

- Composite network agility is a function of both communication and C2-social network agility.

In addition, the following hypotheses will be explored for both the communications and C2-social networks:

- Network quality is a function of network design, network capabilities, and the prevailing conditions determined external to the network (the value of the metrics that are used to determine network value are a function of design, etc.).
- The agility of a network is a function of network design and capabilities.

4.5.1.3 Experiment 1 Metrics

The following are the design parameters, quality metrics, and other variables that will employed in the design and conduct of Experiment 1.

Communication Network Design Parameters

- Communication network capacity will be measured relatively by the degree to which communications bandwidth satisfies expected mission requirements and conditions. This measure involves establishing a benchmark at a capacity level that can satisfy the least demanding case.
- Communications network connectivity will be measured by the links per node. This measure reflects the built-in link redundancy and is related to capacity potential.

Communication Network Q

- QoC will be measured by both absolute and fitness for use measures.
- The absolute measure will be PCMR(t), the probability that the average message sent will be delivered to its intended recipient(s) as a function of time. (average communications network latency can be calculated if desired).
- The fitness for use measure will be the probability that the average[8] measure will be received in a timely manner. This can be calculated for any time requirement given PCMR(t).

Information Network Design Parameters

- While information is being disseminated in Experiment 1, only the communications and social/C2 networks are being simulated. This means that there is no “intervention” or processing that is taking place in the

information network, and hence, no information network design parameters settings. See Experiment 2.

Information Network Q

- QoI will be measured by the access individuals have to relevant information over time (the information needed to perform their assigned tasks). While there is, in effect, no information network intervention taking place, measuring QoI in Experiment 1 provides us with a baseline for future experiments for the case when all of the information network design parameters are set to "none."

C2-Social Network Design Parameters

- C2 approach will be measured by its location in the C2 approach space, its distance from the origin and by its distance from the diagonal.
- Information sharing policy will be determined by the rules governing sharing behaviors and characterized by the importance placed upon sharing.

C2-Social Network Q

- Shared awareness will be measured by the average correctness (correctness being measured by the number of problem pieces that have been solved).
- Timeliness will be measured by the time required to arrive at the first complete, correct solution.
- QoC2 will be measured by a function of shared awareness and timeliness.

Mission requirements, missions difficulty, and conditions and circumstances form the dimensions of the Endeavor Space.

Mission Requirements

- Synchronization challenge will be measured by the level of shared awareness required.
- Time urgency will be measured by the time available to find a solution (first solver).

Mission Difficulty

- Complexity will be measured by the percentage of facts that require no information sharing.
- Contested environment will be measured by how much damage[9] would be sustained were there no cybersecurity measures in place.

Conditions/Circumstances

- Initial information quality will be measured by the ratio of "signal to noise" in the available information. In these experiments, the information necessary to complete the task is available to the enterprise.
- Information richness will be measured by the size of the message required to transmit a piece of information (fact).
- Network damage will be measured by the ratio of damaged links to total links and the ratio of functioning nodes to total nodes
- Cognitive complexity will be measured by the time it takes to process the average fact.

4.5.1.4 Experiment 1 Environment

Experiment 1 is constrained by current capabilities. A review of the capability of available building blocks looked at the parameters that these building blocks could be observed and controlled. Of particular interest were the parameters necessary to instantiate different approaches to C2 and different communications network laydowns. Based upon this review, it was determined that the best option was to lash up the DOD CCRP developed Experimental Laboratory for ELICIT and the NRL-developed (Extendable Mobile Ad-hoc Network Emulator [EMANE]) within ARL's NSRL. Figure 19 is a depiction of this experimentation environment.

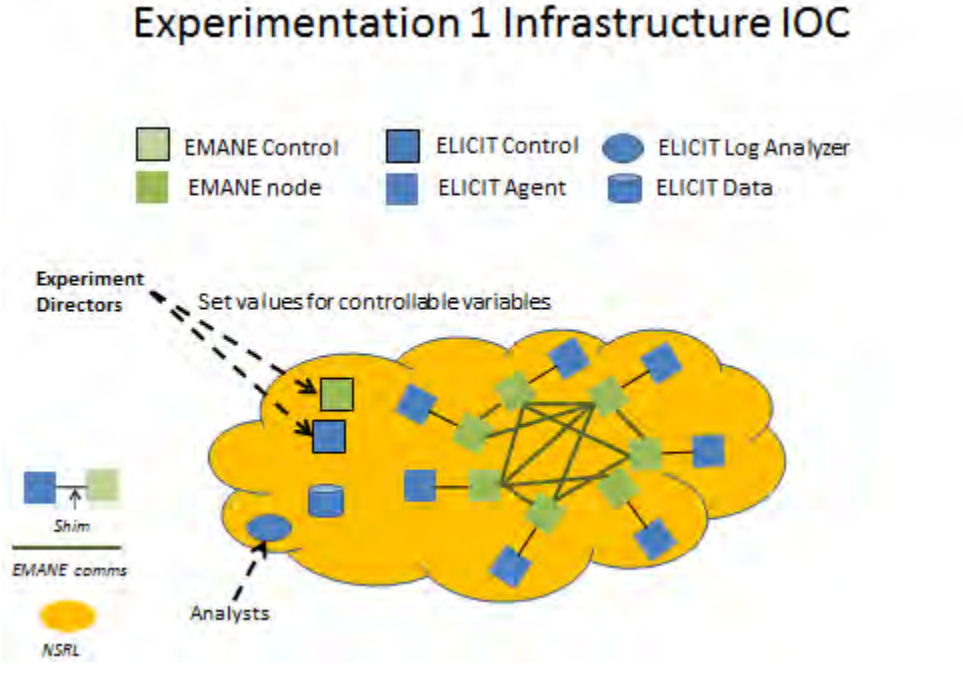

Fig. 19 Environment for Experiment 1

NSRL experimentation IOC capabilities include the following:

- ELICIT implementation of a "social" network whose behavior is shaped by a chosen C2 approach that assigns decision rights, identifies interactions that are "permitted" and determines access to information sources
- EMANE emulation of a communications network where behavior is shaped by the design and capabilities of its access control, physical and shim layers, network topology, and the load that is placed on the network
- ELICIT capability to inject data at various nodes at various times
- ELICIT capability to vary the quality and quality of available data
- ELICIT agent stand-ins for human participants that are have various user configurable parameters that impact decision making
- ELICIT shared awareness task that is user configurable
- Interoperability shim that serves as a "bus" connecting ELICIT and EMANE nodes with the ability to pass messages over either the emulated communication network or an EMANE "back channel." The interoperability shim can also be used to incorporate additional network components through loose coupling.
- ELICIT transaction log generator, data repository, and a log analyzer
- Shim data logging and analysis scripts
- EMANE packet captures (PCAPs) data logging and analysis scripts
- ELICIT and EMANE user interfaces

NSRL IOC capabilities, while providing considerable functionality and flexibility, fall short of the "plug and play" capabilities identified in the NS experimentation vision since they are instantiated for EMANE/ELICIT.

4.5.1.5 Experiment 1 Design

Experiment 1 was designed to accomplish the goal set out in Section 4.5.1.1 by simulating an organization whose objective is to develop correct and timely shared awareness regarding an impending terrorist attack. It involves both a C2-social network that can be instantiated to adopt a variety of C2 approaches including those depicted in Fig. 16 and a tactical mobile communication network that provides connectivity between and among the C2 nodes and information sources. The C2 nodes are represented by software agents whose cognitive capabilities and information seeking and sharing behaviors can be shaped by a variety of

parameters. The parameter default values have been tuned to achieve behaviors that have been observed in ELICIT experiments with human participants.

This experimentation lash-up represents a number of significant interdependencies that exist between a C2 network and the communications network that supports it. Cybersecurity impacts are represented by being able to specify communication network link status and performance capabilities. ELICIT and EMANE provide the data needed to determine QoC and QoC2 and measure task accomplishment. Experiment 1 has been designed to be expanded when the capability to simulate an information network is available and to provide a baseline that can be used to explore the impacts of proposed improvements to network capabilities (e.g., context aware behaviors). Experiment 1 adopts a full factorial design, a design that involves runs that create every unique situation for each treatment combination.

The variables controllable in Experiment 1 include those listed in Fig. 20. The first set of variables collectively determine the integrated design of the 2-genre composite network, while the second set of variables determine the mission characteristics and conditions under which the mission is to be carried out.

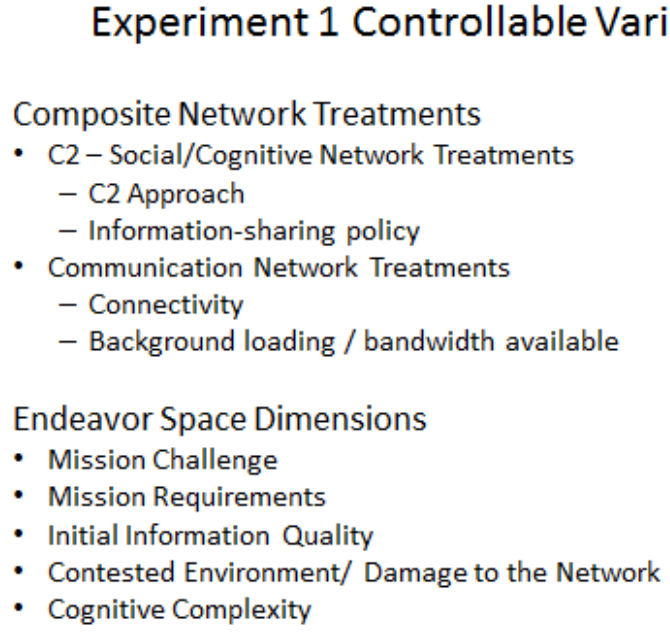

Fig. 20 Experiment 1 controllable variables

The number of values that each of these variables can take on in the experiment determines the minimum number of experiment runs required (1 for each unique combination of variable values). Figure 21 provides the possible values for each mission and circumstances variable. The definition of each of these variables, the values that they take on, and how they are instantiated in the simulated composite network are provided in Appendix A. In combination, these define the Endeavor Space "cells" considered in Experiment 1, where each cell represents a unique

situation. From Fig. 21 we can see that the Endeavor Space is 5 dimensional and contains 1458 cells.

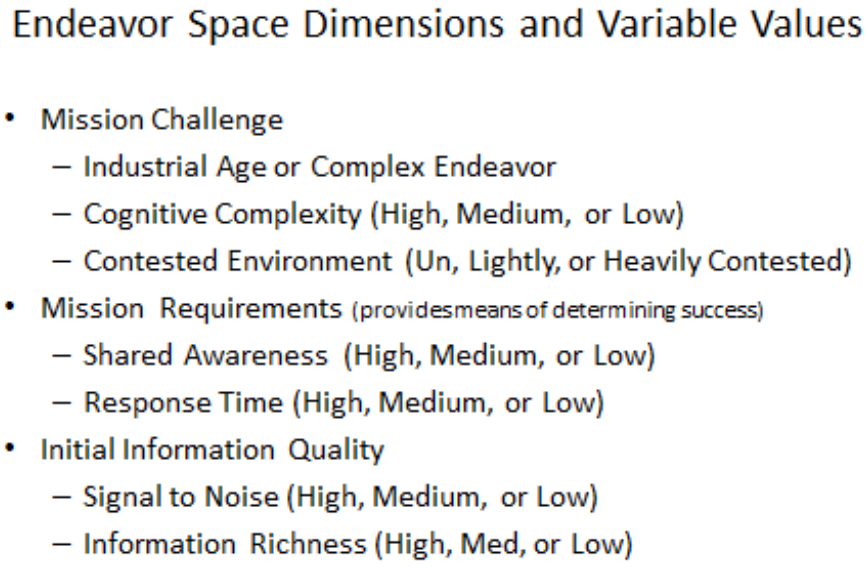

Fig. 21 Endeavor Space dimensions and variable values

The design choices for the composite network that Experiment 1 will consider are identified in Fig. 22. There are 72 possible unique design options for the composite network, options each of which is a unique combination of the design options available for the C2-social network (8), the information network (3), and the communications network (3) that will be explored in Experiment 1.

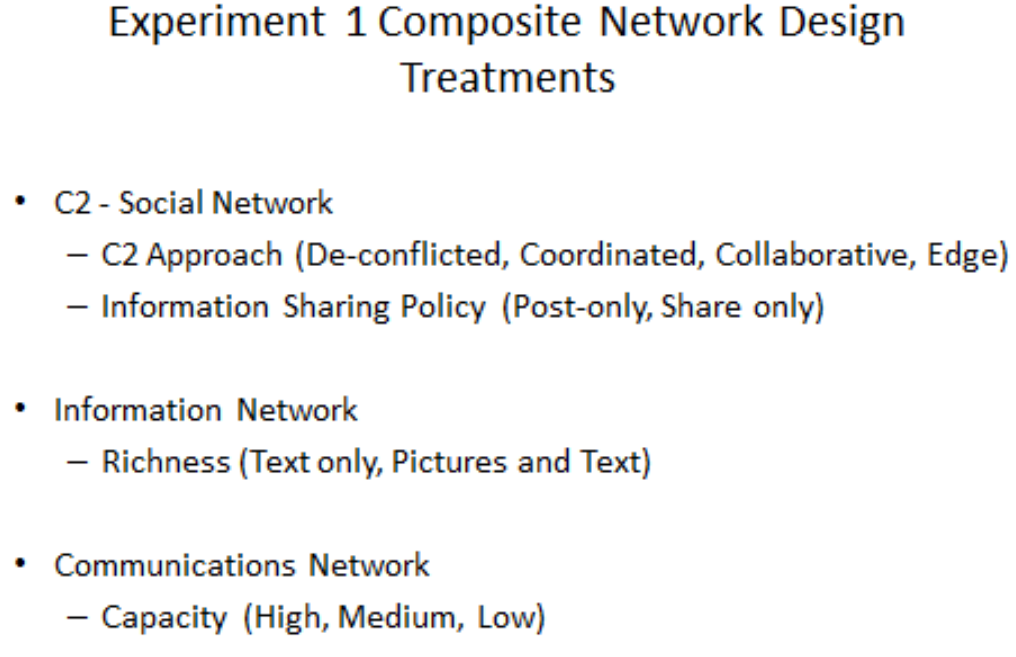

Fig. 22 Experiment 1 composite network design treatments

4.5.1.6 Experiment 1 Run Strategy

With 1458 Endeavor Space cells and 72 composite designs to consider, Experiment 1 would require 104,976 runs to produce at least 1 data point for each unique combination of treatment and condition. Given that we are interested in whether or not a mission succeeds or fails, a "push to fail" strategy that requires far fewer runs can be adopted. This strategy begins with running the least demanding case and then, in subsequent runs increasing the problem difficulty and stresses represented by the Endeavor Space controllable variables until the enterprise fails. After the least demanding run has been completed, each Endeavor Space dimension is stressed in isolation to make sure that the simulation is behaving as expected and to determine the point along each dimension where the mission will fail. The next step is setting up runs that represent a variety of stresses to explore their impacts in a systematic manner, stopping when the level of stress results in mission failure.

The treatment configuration for the least demanding case consists of using a de-conflicted C2 approach with a share-only policy in effect and with only textual messages which minimizes bandwidth requirements. To minimize delays the capacity of the communications network is set to high. The Endeavor Space dimensional parameters are also selected to minimize difficultly and stress as well. Hence, the Industrial Age mission challenge with low cognitive complexity operating in an uncontested communications environment and requiring only low shared awareness and timeliness is used. Information quality is maximized (high signal to noise ratio) to make the circumstances favorable as well. Readers should note that this least-demanding case should result in the best performance and outcomes and serves as an upper bound against which we can measure the relative impact of less favorable circumstances and conditions.

4.5.1.7 Experiment 1 Impacts of Interest

Experiment 1 will, in addition to providing an upper bound for performance, produce results that can be used to investigate the impacts that one variable has on other variables, information that will help us gauge the potential value of proposed improvements in information processing capabilities and the introduction of a capability for context-aware behaviors.

For example, the size of messages exchanged can be reduced by various compression techniques. Decisions about what to compress and when to compress will impact the quality of information delivered as well as the load that information dissemination has on the communications network. In turn, the load on the communication network can affect the frequency and types of interactions between and among individuals and information sources and repositories.

4.5.2 Initial Design for Experiment 2

Experiment 2 is intended to build upon Experiment 1. Experiment 2 requires the addition of a dynamic and interdependent information network layer and a network monitor capability that makes it possible to investigate context-aware behaviors. The design of Experiment 2 is constrained by the capabilities that are expected to be available in the IOC+1 version of the NSRL Experimentation Infrastructure.

4.5.2.1 Experiment 2 Goal

The goal of Experiment 2 is to extend the "proof of concept" to a 3-genre composite network and with it the ability to represent context-aware dynamic network inter-dependencies between and among 3 different networks that involve all 3 genres.

4.5.2.2 Experiment 2 Propositions and Hypotheses

Experiment 2 is designed to build upon the exploration of both the single-genre and composite network hypotheses that were explored in Experiment 1 as well as to explore the following set of additional hypotheses:

- Do context-aware behaviors (having a choice among a set of service options as a function of conditions) improve average quality of network performance and service?
- Under what conditions does the average quality of service improve the most as a result of context-aware behaviors? the least?
- Can context-aware behaviors in the C2-social network and/or information network compensate for degraded performance of the communication network?

4.5.2.3 Experiment 2 Metrics

Experiment 2 adds an information network to the mix, and introduces the concept of context-awareness and the ability to change design parameters as a function of the state of the network(s) involved. Therefore, the following set of design parameters and network quality metrics are needed to augment the design parameters and quality measures employed in Experiment 1.

Information Network Design Parameters

- Information network compression capacity will be measured by the degree to which messages can be compressed without a loss in information as a function of relevance to a particular individual (assume that the same information may provide action information to 1 person and context or queueing information to another. Hence, the amount of loss-less compression would differ depending upon the situation.

Information Network Q

- QoI will be measured by the access individuals have to relevant information over time (information needed to perform their assigned tasks)

4.5.2.4 Experiment 2 Environment

NSRL IOC+1 capabilities feature the addition of an information network and network monitor to provide an opportunity to conduct experiments that are capable of investigating the dynamic inter-dependencies inherent in a composite network capable of context-aware behaviors.

NSRL experimentation IOC+1 capabilities include the following:

- An information network that mediates interactions between the C2-social network nodes and communication network nodes is introduced. The information network nodes contain information agents that can prioritize and compress messages based upon a set of rules that depend upon the sender, the intended recipient and the state of the communication network provided by the network monitor.
- An enhanced ELICIT implementation of a "social" network that it is capable of changing its information sharing policy as a function of its perceived state of the communications network (based upon information provided by the network monitor)
- EMANE emulation of a communications network whose behavior is shaped by the design and capabilities of its access control, physical and shim layers, network topology, and the load that is placed on the network
- An NSRL information network that mediates information dissemination based upon its awareness of the situation (communications network performance and agent information requirements)
- A network monitor that information agents and embedded information processing (information network layer) regarding communications network performance
- ELICIT capability to inject data at various nodes at various times
- ELICIT capability to vary the quality and quality of this data
- ELICIT agent stand-ins for human participants that are have various user configurable parameters that impact decision making
- ELICIT shared awareness task that is user configurable

- Interoperability shim that serves as a "bus" connecting ELICIT and EMANE nodes with the ability to pass messages over either the emulated communication network or an EMANE "back channel." The interoperability shim can also be used to incorporate additional network components through loose coupling.
- ELICIT transaction log generator, data repository, and a log analyzer
- Shim data logging and analysis scripts
- EMANE PCAPs data logging and analysis scripts
- ELICIT and EMANE user interfaces.

Figure 23 is a depiction of the IOC+1 experimentation environment.

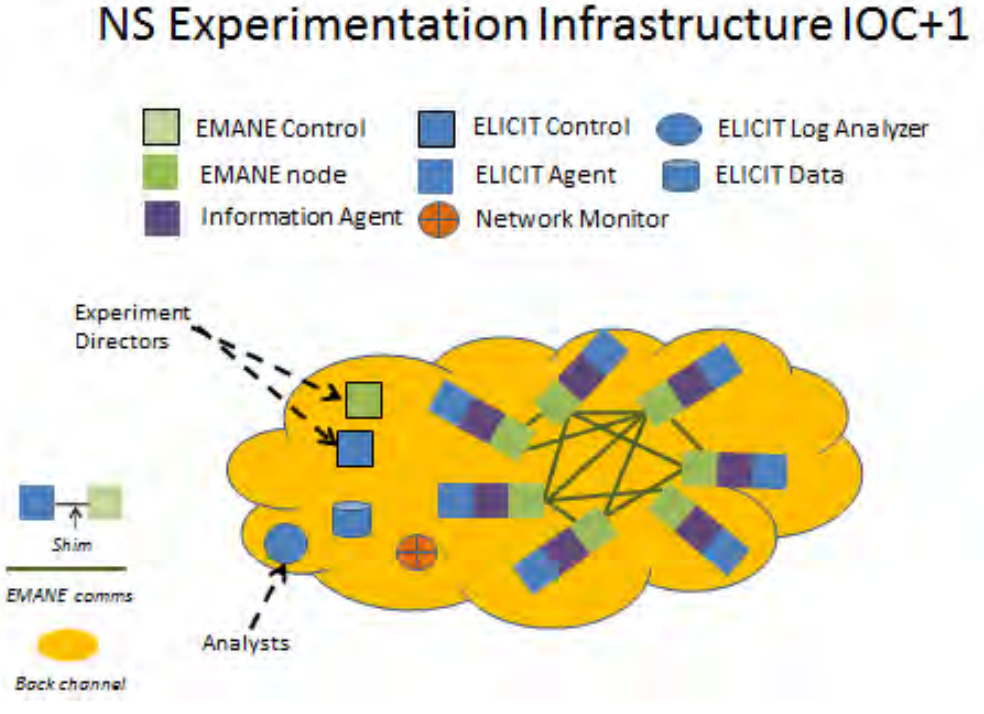

Fig. 23 NS experimentation infrastructue IOC+1

4.5.2.5 Experiment 2 Design

As can be seen in Fig. 24, Experiment 2 introduces 2 additional composite network design parameter values. First, in addition to the 2 enterprise information sharing policy options considered in Experiment 1 (Post Only, Share Only), Experiment 2 will be able to instantiate an adaptive information sharing policy, a policy that can dynamically switch between these 2 policy options as the situation merits informed by the network monitor. Second, the information network layer will have an adaptive option with the capability to dynamically compress pictures or adapt to a

text only mode when the situation merits based upon information provided by the network monitor.

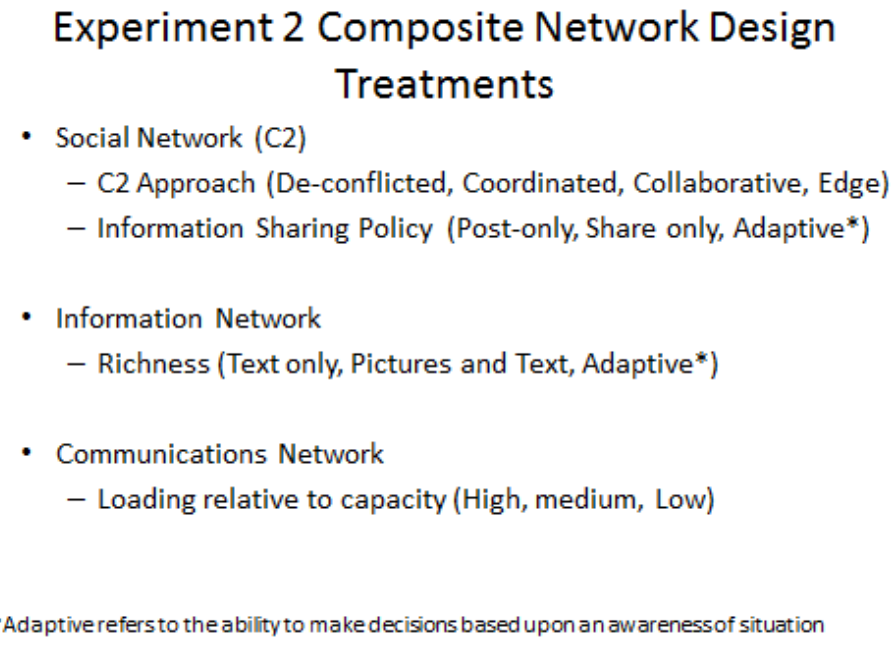

Fig. 24 Experiment 2 composite network design treatments

This brings the number of unique composite network design options to 108 (up from 72 in Experiment 1).

4.5.2.6 Experiment 2 Run Strategy

With 1458 Endeavor Space cells and now 108 composite designs to consider, Experiment 2 would require 157,464 runs to produce at least 1 data point for each unique combination of treatment and condition. Fortunately, we have already run many of these runs in the course of Experiment 1. Since both of the added design options (adaptive information sharing policy and adaptive compression) can be expected to reduce the stress on the communications network, Experiment 2 runs will test to see 1) in cases that involved mission success, where adaptive capability makes sense; and 2) for situations where the mission failed, whether having an adoptive option turns failure into success.

4.5.2.7 Experiment 2 Impacts of Interest

Experiment 2 will produce results that can be used to investigate the potential of context-aware adaptive capabilities to provide higher levels of performance and increase agility. For example, Experiment 2 will tell us how much of a performance penalty is paid by introducing a network monitor and adaptive capability (a monitor increases communications traffic a, ties up computational resources, and increases cognitive). Experiment 2 will also help to tell us whether the expected benefits in

overall composite network agility materialize despite these costs, and if so, for which mission challenges and under what conditions.

4.5.3 Concept for Experiment 3

Experiment 3 involves a significant enhancement to the CAMPX's ability to incorporate cybersecurity capabilities into the experimentation environment and with this capability, an ability to address cyber-defense design issues and tradeoffs involving cyber-defense and cyber-related risks in the context of the overall composite network. The design of Experiment 3 is constrained by the capabilities that are expected to be available within 2 years. For the purposes of this report, it was assumed that there would not be an ability to interconnect the NSRL with the CSTB within this period and that with 1 exception, that these 2 capabilities would not be capable of plug and play operations. This 1 exception was that, based upon currently available information, ELICIT capabilities could be instantiated in the CSTB. Thus, it would be practical to design an experiment that employed parallel environments, using the results of 1 to set parameters in the other. If this turns out not to be the case, the initial design of Experiment 3 proposed here should be revisited.

4.5.3.1 Experiment 3 Goal

The goal of Experiment 3 is to further extend the "proof of concept" to a composite network that integrates agile cyber-defense capabilities and with it the ability to explore and assess cybersecurity strategies and capabilities in the context of a militarily relevant 3-genre composite network. This also extends network "awareness" to the cybersecurity related states including the nature of attack-vectors, the performance of defensive measures, and the resulting state of the various networks.

4.5.3.2 Experiment 3 Propositions and Hypotheses

Experiment 3 is designed to build upon the exploration of both the single-genre and composite network hypotheses previously explored in Experiments 1 and 2 to ascertain the impacts of cybersecurity capabilities in an Endeavor Space that is augmented to include a more granular set of cybersecurity conditions.

The data provided by Experiment 3 will be used to determine the extent to which there is empirical support for the following hypotheses:

- A balanced, integrated cybersecurity design (one that takes into consideration cross-genre tradeoffs) minimizes the adverse impacts of cyber attacks.

- A context-aware cybersecurity capability reduces the costs of cyber defense while maintaining or improving composite network performance and agility.
- The enhanced agility (provided by cybersecurity capabilities) of 1 or more networks compensates for a lack of defensive capability or adversary over-match in other networks.

4.5.3.3 Experiment 3 Metrics

In addition to the metrics previously employed in Experiment 1 and 2, Experiment 3 will involve a set of cybersecurity-related parameters and associated metrics (to be developed in conjunction with the Communications-Electronics Research, Development and Engineering Center [CERDEC]) related to the following:

- Adversary cyber capabilities
- Communication network cybersecurity capabilities
- Information network cybersecurity capabilities
- C2 – social network cybersecurity capabilities
- Cyber awareness.

4.5.3.4 Experiment 3 Environment

Experiment 3, with its focus on the impacts of cybersecurity capabilities, requires establishing parallel environments (ARL's NSRL and its CSTB) with a common "C2-social" network as depicted in Fig. 25. Moving from IOC+1 to IOC+2 involves the creation of a CSTB, currently under development, a network monitor that provides the state of the networks that are represented, and the instantiation of ELICIT agents and the ELICIT environment in the CSTB. Experiment directors will now have access to both NSRL and CSTB control where they can specify Endeavor Space conditions, C2 approach options, and cyber-defense capabilities and attack scenarios.

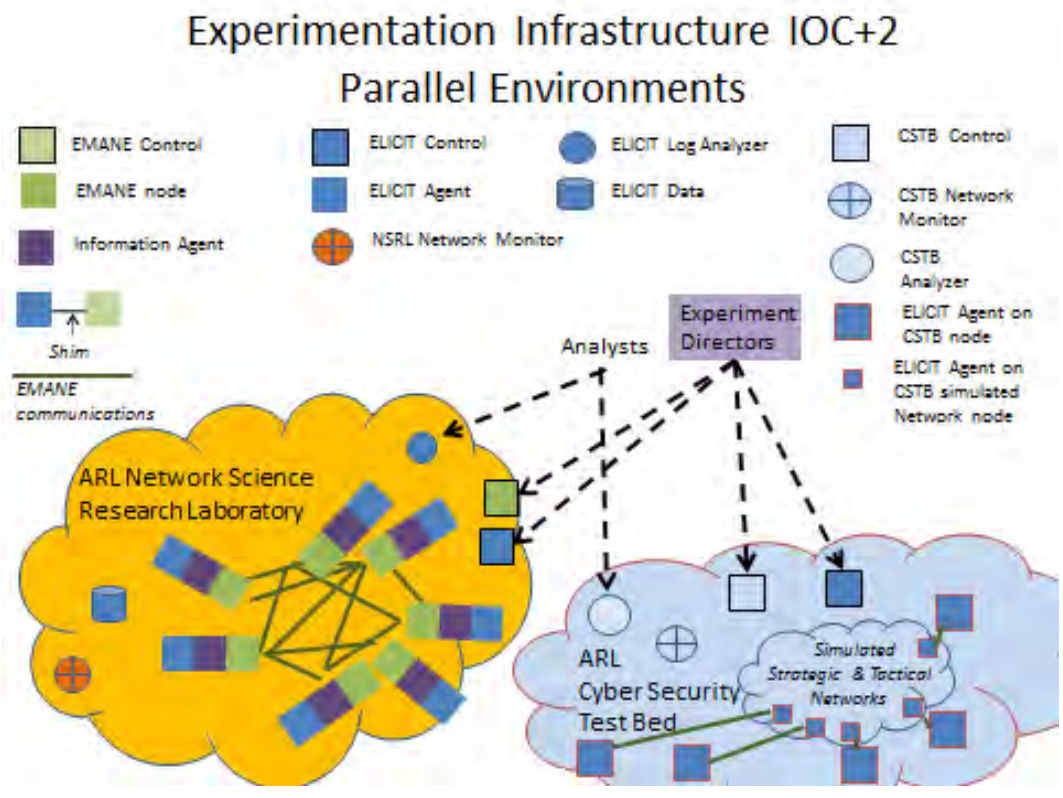

Fig. 25 NS experimentation environment IOC+2

4.5.3.5 Experiment 3 Design

As can be seen in Fig. 26, Experiment 3 introduces a fourth design parameter, cybersecurity, with 4 treatment options.

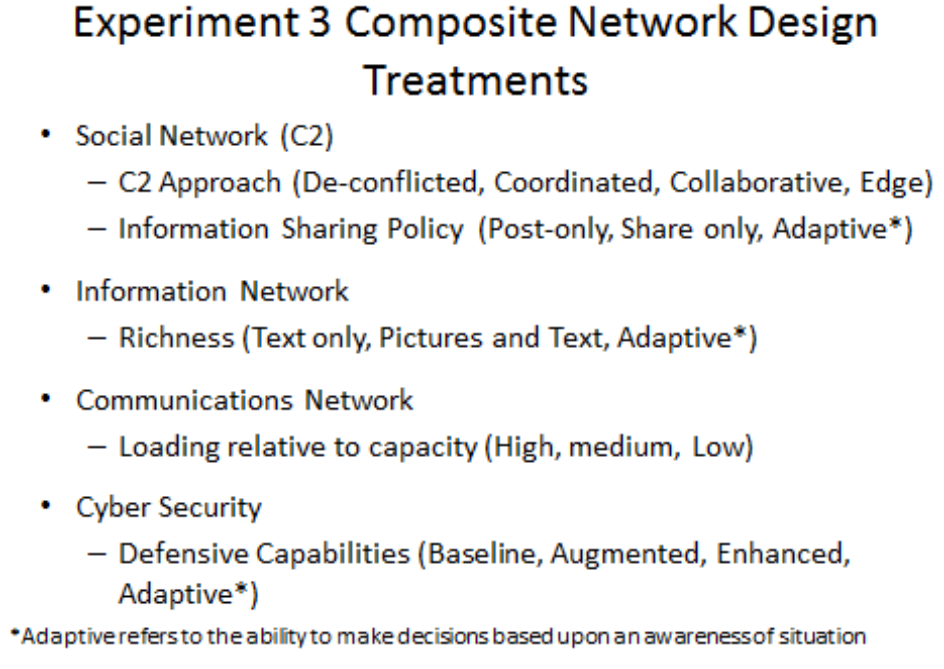

Fig. 26 Experiment 3 composite network design parameters

4.5.3.6 Experiment 3 Run Strategy

With 1458 Endeavor Space cells and 432 composite designs to consider, Experiment 3 would require over a half a million runs to produce at least 1 data point for each unique combination of treatment and condition. Since even in an uncontested environment, cybersecurity measures may have benefits, for example, protection against system failures, a baseline that can serve as a basis for comparison, first needs to be established. Thus, Experiment 3 runs will begin with establishing how each cybersecurity treatment option performs in an uncontested environment for different mission challenges and conditions. As in previous experiments, many runs do not need to be made. In cases where, for a given cybersecurity treatment, the mission does not succeed, there would be no need to do experimental runs for more stressful situations.

4.5.3.7 Experiment 3 Impacts of Interest

Experiment 3 will produce results that can be used to investigate the interplay between the risk avoiding and risk mitigating that cybersecurity offers and the performance and agility of the composite network. Analysis of experiment runs will enable us to better understand the advantages and disadvantages of various approaches to cybersecurity and cybersecurity policy options under a variety of mission challenges and conditions. The dynamics of adaptive cybersecurity capabilities and their interactions with context-aware behaviors in the composite network will inform efforts at integrated design. Experiment 3 is the first of a critical thread of experimentation; one that enables us to understand composite networks under the kinds of cyberattacks deployed military forces need to anticipate and operate.

5. Way Ahead

A number of ARL staff and researchers associated with the NS CTA and the CS CRA have been part of the discourse that ultimately culminated in this articulation of an Experimentation Ecosystem and CAMPX. These conversations have resulted in a number of efforts to design and conduct experiments that, to varying degrees, instantiate a composite network and explore related hypotheses. These efforts have begun to produce results. These efforts have also resulted in 2 papers that have been accepted for the 20th International Command and Control Research Symposium.[10] The following 2 papers describe the experiments that have been designed, the experimentation environment that instantiates a composite network, and preliminary results:

- Kevin Chan and David Alberts, “Exploring Composite Network Agility”

- Lisa Scott, Kevin Chan, Will Dron, Alice Leung, David Alberts, “Modeling Information Propagation in Overlapping and Adaptive Social, Information, and Communication Networks”

The experimental capabilities developed to date significantly improve the ability of researchers to instantiate militarily composite networks and conduct research that explores the interdependencies between and among the constituent networks. It is expected that these capabilities will be built upon by NS CTA, CS CRA researchers, as well as others over the coming years. The extent to which this actually occurs will depend, in large part, upon the direction ARL provides to its ongoing initiatives and the priority it places upon the development of environments that can instantiate and instrument composite networks.

6. References and Notes

1. Case Studies and experiments that support this conclusion can be found in the following four publications: SAS-065 NATO NEC C2 Maturity Model (CCRP Press 2010); The Agility Advantage (CCRP Press 2011); NATO SAS-085 C2 Agility Final Report (NATO SAS 2014) and C2 Re-envisioned: The Future of the Enterprise (CRC Press 2015).

2. Kott A, Alberts D, Zalman A, Shakarian P, Maymi F, Wang C, Qu G. Visualizing the tactical ground battlefield in the year 2050: workshop reports. Adelphi (MD): Army Research Laboratory (US); June 2015. Report No.: ARL-SR-0327

3. These projects were identified by Alice Leung from BBN.

4. The term average as used here do not preclude a decision maker from attaching a relative value to each instance of mission, circumstance, and condition rather than assuming that all are equally likely or importance to make the measure of agility a weighted average.

5. Infostructure refers to the infrastructure necessary to support communications and information capabilities.

6. Alberts' The Agility Advantage (2011) identifies 6 enablers of agility including responsiveness, resilience, versatility, flexibility, adaptability, and innovativeness. Having a network monitor makes it possible for a system to be, for example, more responsive and resilience. This, in turn, can increase agility.

7. In this report, the unit of measurement for communications is a message rather than a packet. A more granular look at communication network performance would focus at the packet level and PCMR(t) at the message level could be calculated or directly observed.

8. In the experiments proposed, there are messages of different sizes.

9. How one can measure damage depends upon the nature of the attacks that are being simulated. One example of a measure of damage include percent of loss links, nodes, and messages. These losses will affect behaviors and outcomes.

10. The proceedings (in the form of a collection of peer reviewed papers) will be become part of the CCRP archives.

Appendix A. Composite Network Simulation Variables & Values

A-1 Introduction

The composite network simulation environment needed to support Experiment 1 consists of the following 3 major components:

- an NRL-developed mobile communication network emulator (EMANE)
- the DOD CCRP-developed experimentation environment, ELICIT
- a NS CTA-developed shim and simulation component integration interface.

EMANE is used to simulate a communications network, ELICIT simulates both a C2-social network and a set of information sources and the shim mediates control and data flows between and among the representations of the single-genre networks. Both EMANE and ELICIT possess sets of parameters that permit researchers to design the communications and C2-social networks involved. ELICIT is capable of human-in-the-loop or agent-based experimentation.

Experiment 1 involves agents (representing humans) who are organized into n person teams. The various C2 approaches that can be instantiated in this set of experiments serve to shape agent behaviors. Different C2 approaches are instantiated by the assignment of roles and responsibilities, the specifications of individuals' interactions with one another, and information accesses. This is accomplished by configuration files. Agent capabilities and behaviors are shaped within the context of a given C2 approach by choosing parameter values in an agent configuration file. ELICIT is also capable of varying the nature and difficulty of the mission challenge. Experiment 1 also involves a communications network whose bandwidth is configurable by setting the value of a parameter.

A-2 Experiment 1 Run Setup

To set up an Experiment 1 run, a researcher simply needs to edit a script file to select the set of configuration files needed. If appropriate, these configuration files can be modified to further tailor the run to the experimenter's requirements. To start a run, the following command is used: - run_test.sh elicit.scn

The contents of run_test.sh, elicit.scn, and the ELICIT batch and configuration files needed are provided below. Please note the all lines that begin with # (# ……) are ignored by the computer and serve as comments or are a way of providing options to researchers who only need to comment out the parameter value and uncomment out a new value to prepare for another run.

A-2.1 run_test.sh

```
export XCN_ROOT=`(cd ../xcn && pwd -P)`

SCN=`pwd`/$1
if [ ! -f "$SCN" ]; then
 echo "Must supply a scenario file as the first argument:"
 echo "$0 <scn file>"
 exit 1
fi

export CONFIG=$XCN_ROOT/nodes.config

if [ ! -d "$XCN_ROOT" ]; then
 echo "Could not find XCN_ROOT=$XCN_ROOT"
 exit 1
fi

CWD=`p
```

run_test.sh

```
wd`
cd$XCN_ROOT
ln-f -s $CWD .


# stop all existing emane/ns3/core
./kill.sh -f
sleep 1


#run the scenario
source ./start_scenario_core.sh $SCN $CONFIG
```

A-2.2 elicit.scn

```
#! /bin/bash

export XCN_ROOT=`(cd ../xcn && pwd -P)`

SCN=`pwd`/$1
if [ ! -f "$SCN" ]; then
 echo "Must supply a scenario file as the first argument:"
 echo "$0 <scn file>"
 exit 1
fi

export CONFIG=$XCN_ROOT/nodes.config

if [ ! -d "$XCN_ROOT" ]; then
```

```
 echo "Could not find XCN_ROOT=$XCN_ROOT"
 exit 1
fi

CWD=`pwd`
cd $XCN_ROOT
ln -f -s $CWD .

# stop all existing emane/ns3/core
./kill.sh -f
sleep 1

# run the scenario
source ./start_scenario_core.sh $SCN $CONFIG
wdron@xcn3:/home/wdron/experimentation/Emulation_Experiments/elicit$ more
elicit.scn
#! /bin/bash

ELICIT_DIR=$(cd ../../Tools/elicit && pwd -P)

export OUTPUT_DIR="$HOME/sim_runs/elicit"

# this is overwritten if we use a mobility file
NUM_NODES=17

# EMANE scenario has 25 nodes, so we have to ignore 8 of them (these were
decided
# from the camp roberts scenario
ELICIT_IGNORE_NODES="0 1 10 11 16 18 20 21"

# pick 4 nodes to act as websites
ELICIT_WEBSITES="0 10 16 21"

# note we run until the elicit trial is done, so we ignore duration
DURATION=9999

export EMANE_RADIO="rfpipe"
export TXPOWER=-6
if [ -z "$BANDWIDTH" ]; then
 export BANDWIDTH=250000
 #export BANDWIDTH=100000

fi

# wifi
#export EMANE_RADIO="Ieee80211abg"
#if [ -z "$BANDWIDTH" -a -z "$TXPOWER" ]; then
# #export BANDWIDTH=1000000; export TXPOWER=-20
```

```
# #export BANDWIDTH=500000; export TXPOWER=-23
# #export BANDWIDTH=100000; export TXPOWER=-30
# export BANDWIDTH=50000; export TXPOWER=-33
#fi

if [ -z "$MOBILITY" ]; then
 #MOBILITY="`pwd`/elicit/configs/25node-linear.mob"
 MOBILITY="`pwd`/elicit/configs/25node-grid.mob"
 fi

export STATIC_ROUTES="`pwd`/elicit/configs/`basename $MOBILITY
'.mob'`.onehops"

if [ -z "$ELICIT_BATCH" ]; then
 #ELICIT_BATCH="`pwd`/elicit/configs/elicit-17nodes/agent-batch-
BASELINE-Indust
rialAge-Hierarchy-shareonly.txt"
 ELICIT_BATCH="`pwd`/elicit/configs/elicit-17nodes/agent-batch-BASELINE-
EDGE-sh
areonly.txt"
fi

source ../shim/shim_exp.scn
```

A-2.3 ELICIT Batch File for Baseline EDGE Share-only C2 Approach

```
<start trialset>
interval|5
waves|3
trial|120|factoidset1a5-17.txt|countries1.txt
names|names17.txt
group|organization-BASELINE-EDGE-shareonly-17.txt
ncsconffile|NCSConf_SimpleNCS2.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
```

role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
role|SenseMaking_Agent2.4_shareonly.txt
agentauditing|off
teamtableauditing|off
numberofidentifies|-1
natureOfParticipants|agent
experienceOfParticipants|agent
baselineExperiment|yes
ncsRecheckShareQueueDelay|0

This batch file specifies all of the configuration files as well as a number of other parameters needed to set up ELICIT for a run. The first 2 parameters determine the timing of information entering the organization (information will be distributed in 3 waves 5 min apart. The next parameter specifies the length of the run, which is in this case 120 min (simulation time).

The factoid set file (factoidset1a5-17.txt|countries1.txt) contains the list of facts that will be disseminated and specifies, for each factoid, the subject and importance of the factoids, to which it will be "sent," and in which wave as well as the factoid itself and its size in bytes. An example of the specification for a fact is

1|E|1|2|1|1|The Lion is involved (20000 bytes)

The 6-part code at the beginning of this factoid provides a unique identifier for the fact as well as information about how it is to be distributed. The factoid key is interpreted as follows:

- The first number in the key is the number of the factoid in the factoid set, in this case this is the first factoid in the set.
- The second part of the key indicates the importance or impact of the fact [E, K, N, or S], where E factoids represent expert information as in this example, K factoids represent key information, N factoids are noise. They are not important. The game can be correctly solved if these are ignored. S factoids are supportive. These factoids support the information in the E and K factoids. Any character can be used. The sensemaking agents rely on the E and K designations to make some decisions about sharing important factoids.
- The third part of the key specifies what primary subject of the factoid or Fact Type [1 is Who as in this case, 2 is What, 3 is Where and 4 is When]. Some factoids contain information that is useful for solving more than 1 subproblem but only the primary type is specified.

- The fourth part of the key specifies to whom (the individual or agent or website) the factoid will be sent, in this case, individual 2.
- The fifth part of the key specifies the wave in which the factoid will be distributed, in this case, the first wave. The count of the factoid within its type-impact category. This count makes the factoid keys unique.
- The last part of the factoid key specifies the number in the factoid set since some factoids can be repeated in order to send them to different individuals and/or at different times.

The organization file specifies the nature of the organization to be created and C2 approach to be employed. It specifies the number of individuals and websites (if any), the roles and responsibilities of each individual, who can directly interact with whom, and who has access to each website. This organization file (organization-BASELINE-EDGE-shareonly-17.txt) is a 17-person edge organization where individuals share directly with one another (without posting or pulling from websites).

The batch file continues with the specification of the agent files, one for each "person" contained in the organization file and concludes with a number of other parameters that determine what information is generated during the run and some run metadata. The agents developed for ELICIT possess a number of parameters that determine their cognitive abilities and shape their behaviors. The ELICIT Software Guide that can be found at

http://www.dodccrp.org/files/ELICIT_2.5_Software_Guide_August_2011.pdf

This batch file uses the same agent file for all organization members. The meanings of the different agent parameters settings are explained in the software guide. The other agent parameters are set to their default values.

INTENTIONALLY LEFT BLANK.

Appendix B. The Quest for Key Information: Does C2 Approach Matter?

The paper, The Quest for Key Information: Does C2 Approach Matter? (Alberts, D.S. and Vassiliou, M) can be found at

http://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/54da583ee4b0fd1bf8e20f9e/1423595582718/017.pdf

List of Symbols, Abbreviations, and Acronyms

ALC	Adelphi Laboratory Center
AREP	Applied Research and Experimentation Partner
ARL	US Army Research Laboratory
ARO	Army Research Office
BDA	battle damage assessment
C2	command and control
CAMPX	campaign of experimentation
CERDEC	Communications-Electronics Research, Development and Engineering Center
CCRP	command and control research community
Co-EDIN	Co-evolution and Dynamics of Inter-genre Networks
CS CRA	Cybersecurity Collaborative Research Alliance
CSTB	Cybersecurity Test Bed
DES	discrete event simulator
DOD	Department of Defense
ELICIT	Experimental Laboratory for the Investigation of Communications Information-sharing and Trust
EMANE	Extendable Mobile Ad-hoc Network Emulator
Exp	Experimentation
IOC	Initial Operational Capability
IPAN	Information Processing Across Networks for Decision-Making
MoEs	measures of effectiveness
MoPs	measures of performance
MORS	military operations research
NS CTA	Network Science Collaborative Technology Alliance
NSRL	Network Science Research Laboratory
OD	organizational design

PCAP	packet capture
Q	quality
QoC	quality of communications
QoC2	quality of C2
QoCS	quality of cybersecurity
QoI	quality of information
QoI-SAN	Quality of Information for Semanticaly Adaptive Networks
R&D	research and development
SMEs	subject matter experts
TIME	Trust, Influencing, Modeling & Enhancing Human Performance

1 (PDF) DEFENSE TECHNICAL INFORMATION CTR DTIC OCA

2 (PDF) DIRECTOR US ARMY RESEARCH LAB RDRL CIO LL IMAL HRA MAIL & RECORDS MGMT

1 (PDF) GOVT PRINTG OFC A MALHOTRA

5 (PDF) DIRECTOR US ARMY RESEARCH LAB RDRL CIN ALEXANDER KOTT BRIAN RIVERA KEVIN CHAN LISA SCOTT REGINALD HOBBS

1 (PDF) INSTITUTE FOR DEFEN ANALYSIS DAVID ALBERTS

2 (PDF) BBN ALICE LEUNG WILL DRON

1 (PDF) VENCORE LABS INC RITU CHADHA

INTENTIONALLY LEFT BLANK.